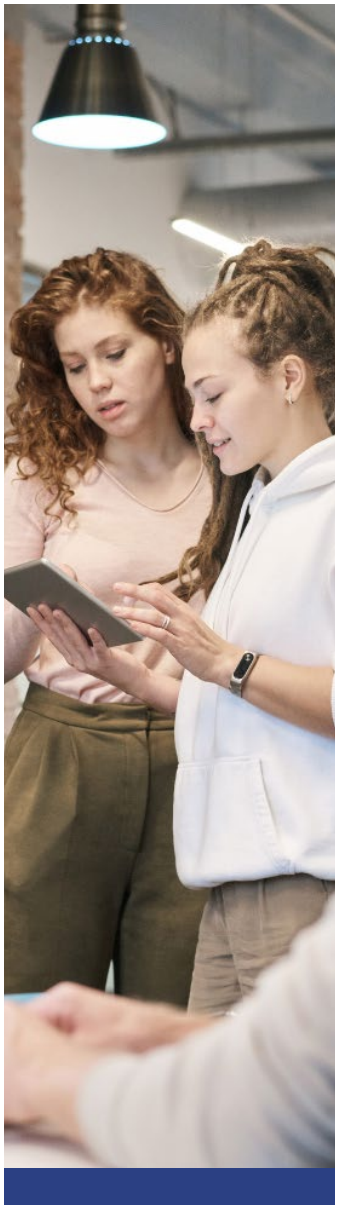
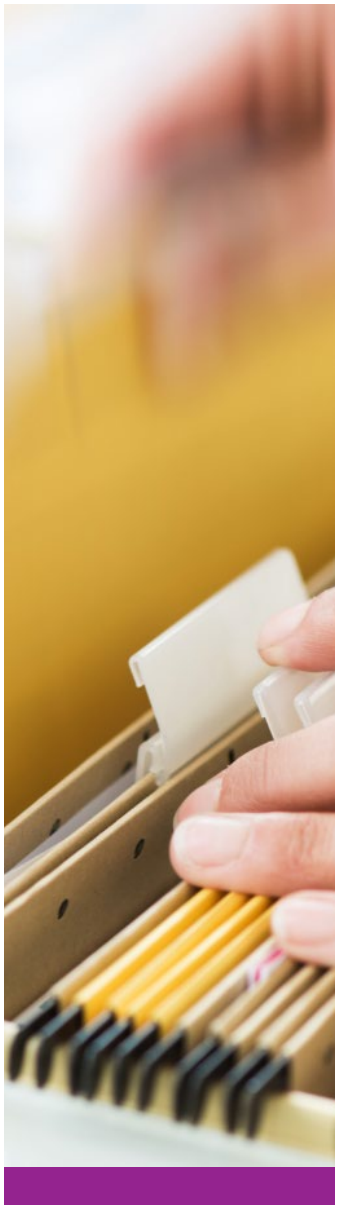
Privacy Compliance Manual

APRIL 2025

A manual for schools that are members of an association of Independent schools and schools and systems that are represented by the National Catholic Education Commission.



INDEPENDENT SCHOOLS AUSTRALIA

NATIONAL CATHOLIC EDUCATION COMMISSION

ME_206281805_9

About this Manual and How to Use it

The Privacy Compliance Manual (updated to 2025) supersedes the Privacy Compliance Manual, first published in 2001 and updated at various times. Therefore, you should discard previous versions of the Manual.

The Manual's purpose is to assist and guide non-government schools with the requirements they must observe concerning preserving an individual's privacy.

The preparation of The Manual has focused on visual presentation and content structure to make it more accessible. In some areas, the content has been amended.

The Manual is in 5 Parts:

Part A: An overview of privacy regulation in schools.

Part B: Data breach response and Notifiable Data Breach procedures.

Part C: Common privacy issues and scenarios that arise for schools.

Part D: The Australian Privacy Principles in detail.

Part E: Annexures, templates and policy documents for school use.

Including a specific section relating to data breach is in response to increasing cyber security threats and the requirements to prepare and respond appropriately. There are now substantial penalties for serious or repeated privacy infringements apart from the reputational damage a school may suffer due to a breach.

There is also a specific section relating to the use of AI in schools and template Privacy and Collection Notices have been amended to take this into account

We recommend all school staff to be aware of the topics covered in Part A. In addition, the privacy officer or person responsible for privacy in a school should be familiar with Parts B and C.

Independent Schools Australia and National Catholic Education Commission have jointly funded the preparation of this Manual.

DISCLAIMER

This Manual is for guidance only. Individual schools and systems may wish to seek specific advice on how to comply with the Privacy Act and other applicable legislation.

Privacy Compliance Manual

STRUCTURE OF THE MANUAL

The revised manual is in 5 parts:

Part A

An overview of privacy regulation in schools.

Part B

Data breach response and Notifiable Data Breach procedures.

Part C

Common privacy issues and scenarios that arise for schools.

Part D

The Australian Privacy Principles in detail.

Part E

Annexures, templates and policy documents for school use.

Part A

Overview of privacy obligations as they apply to Schools

Part B

Responding to data breaches

Part C

Particular issues for Schools

Part D

Explanation of APPs as they apply to Schools

Part E —

PART A

Overview of privacy obligations as they apply to Schools

1. Introduction

Background - The Privacy Act 1988

Health Records

Australian Privacy Principles

To whom does the Privacy Act apply?

2. Summary of a School's Obligations under the APPS

3. Guidelines for Ensuring Compliance

4. Information Covered by the Privacy Act

Types of information covered

What is 'personal information'?

What is 'sensitive information'?

What is 'health information'?

What is a 'record'?

Which acts and practices are exempt?

5. Examples of Information Collected and Held by Schools

Personal information likely to be collected

Sensitive information likely to be collected

1. INTRODUCTION

Background - The *Privacy Act* 1988

1.1 The *Privacy Act* 1988 is a Commonwealth Act that regulates the collection, storage, use and disclosure of different types of personal information by:

(a) Commonwealth and Australian Capital Territory government agencies; and

(b) private sector organisations (i.e., Schools) with turnovers of over $3 million.

1.2 This Manual sets out a guide for Schools in handling the personal information of students, parents, employers and other people. In the Manual, the *Privacy Act* 1988 is referred to as the 'Privacy Act'.

Health Records

1.3 Specific legislation applies in various States and Territories imposing certain limitations on how an organisation may deal with health records.

1.4 This legislation applies in New South Wales, Victoria and the Australian Capital Territory.

1.5 The obligations which apply in respect of health records are set out in Part C at Section 2.

Australian Privacy Principles

1.6 A key component of the Privacy Act is the mandatory requirement for a School to comply with the Australian Privacy Principles (**APPs**). The APPs set minimum standards which relate to the collection, security, storage, use, correction and disclosure of personal information and access to that information. The APPs are summarised individually throughout this Manual, and briefly summarised in Section 2 of this Part. In addition, a detailed explanation of each APP is contained in Part D.

1.7 The Privacy Act also includes mechanisms enabling individuals to:

(a) make complaints about the handling of their personal information; and

(b) receive compensation for interferences with their privacy.

1.8 Schools must comply with the APPs. If a School is found to interfere with a person's privacy, the Office of the Australian Information Commissioner (**OAIC**) can make a declaration that there has been an interference with a person's privacy, that compensation or damages should be paid to that person, that the School publish a statement about the conduct, and/or that the School take steps to ensure it does not occur again. The OAIC can also require a School to give enforceable undertakings that it will take or refrain from taking specified actions so as to comply with the Privacy Act or take specified actions to ensure that it does not interfere with the privacy of an individual in the future. It is possible for substantial pecuniary penalties to be imposed if there is a serious or repeated interference with a person's privacy.

To whom does the Privacy Act apply?

1.9 Under the Privacy Act, both Commonwealth agencies and private sector organisations, including most non-government schools, are regulated by the APPs. The concept of an 'APP Entity' is used in the APPs to cover both types of entities.

1.10 There are some types of entities which will be exempt from the application of the Privacy Act. These are discussed in Paragraph 4.8 of this Part.

2. SUMMARY OF A SCHOOL'S OBLIGATIONS UNDER THE APPS

Obligation	Manual Ref.
Manage personal information in an open and transparent way.	Part D at Paragraph 1.1
Take reasonable steps to implement practices, procedures and systems (including staff training) relating to the School's functions or activities that: • will ensure compliance with the APPs; • will enable the School to deal with inquiries or complaints about compliance with the APPs.	Part D at Paragraph 1.3
Have a clearly expressed and up-to-date Privacy Policy about the School's handling and management of personal information.	• Section 1 of Part C • Part D at Paragraph 1.12 • Sample privacy policies in Annexure 5
If it is lawful or practicable, give individuals the option of interacting anonymously with the School or using a pseudonym (e.g., parents making enrolment enquiries).	Part D at Section 2
Only collect personal information that is reasonably necessary for the School's functions or activities.	Part D at Paragraph 3.4
Obtain consent to collect sensitive information unless specified exemptions apply.	• Part D at Paragraph 3.57 • See also Section 7 of Part C
Use fair and lawful means to collect personal information.	Part D at Paragraph 3.10
Collect personal information directly from an individual if it is reasonable and practicable to do so.	Part D at Paragraph 3.5
If the School receives unsolicited personal information, determine whether the collection is reasonably necessary for its functions and activities. If so, APPs 5-13 (summarised below) will apply. If not, the information must be destroyed or de-identified.	Part D at Paragraph 3.72
At the time the School collects personal information or as soon as practicable afterwards, take such steps (if any) as are reasonable in the circumstances to make an individual aware of the following (e.g., through a privacy collection notice): • why the School is collecting information about them; • who else the School might give it to; and • other specified matters.	• Section 1 of Part C • Part D at Paragraph 3.25 • Sample privacy collection notices in Annexure 5.
Take such steps (if any) as are reasonable in the circumstances to ensure the individual is aware of this information even if the School has collected the personal information from someone else.	Part D at Paragraph 3.25

Obligation	Manual Ref.
Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in APP 6.2 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances).	Part D at Section 4
If the information is sensitive, the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the primary purpose of collection.	Part D at Section 4
Do not use personal information for direct marketing (including for fundraising), unless one of the exceptions in APP 7 applies (for example, the School has obtained consent or where the individual has a reasonable expectation of their information being used or disclosed for that purpose and the School has provided a simple means for the individual to unsubscribe from such communications).	Part D at Section 4
Before the School discloses personal information to an overseas recipient it must take reasonable steps to ensure that the recipient does not breach the APPs, unless an exception applies.	Part D at Section 6
Government related identifiers (e.g., driver's license or Medicare number) must not be adopted, used or disclosed unless one of the exceptions applies (e.g., the use or disclosure is reasonably necessary to verify the identity of the individual for the purposes of the School's functions or activities).	Part D at Section 7
Take such steps (if any) as are reasonable in the circumstances to ensure the personal information the School collects, uses or discloses is accurate, complete and up-to-date and, in respect of use or disclosure, relevant. This may require the School to correct the information and possibly advise organisations to whom it has disclosed the information of the correction.	Part D at Section 8
Take reasonable steps, including technical and organisational measures, to protect the personal information the School holds from misuse, interference and loss and from unauthorised access, modification or disclosure.	Part D at Section 9
Take reasonable steps to destroy or permanently de-identify personal information no longer needed for any purpose for which the School may use or disclose the information (provided the School is not legally required to retain the information).	Part D at Section 9.21
If requested by the individual, the School must give access to the personal information it holds about the individual unless particular circumstances apply that allow it to refuse or limit the extent to which it gives access.	• Part D at Section 10 • Section 5 of Part C
Where a data breach occurs take immediate steps to contain the breach and prevent reoccurrence. If it may cause serious harm to an individual, advise the individual and the OAIC.	• Part B • Annexure 1 – Annexure 3

Note: This is a summary only and NOT a full statement of obligations.

3. GUIDELINES FOR ENSURING COMPLIANCE

How to comply with the Privacy Act*

The School should consider using the following action plan in taking steps to comply with the Privacy Act:

3.1 Consider appointing a **privacy officer** or other person who will be responsible for privacy related issues.

3.2 **Internal review of information handling:**

map and regularly review current information handling practices and security procedures. This may involve the privacy officer (or other person) engaging with relevant School employees who collect, use, disclose, or assist the School in protecting (e.g., IT staff), personal information. For guidance, see the privacy planning template in Annexure 4.

3.3 Analyse results of internal review to identify:

(a) what personal information the School collects, about whom and from whom;

(b) whether the School is required by law to collect any of the personal information;

(c) why the School collects and uses personal information;

(d) to whom the School discloses personal information and why, including disclosures to related bodies corporate, and whether any recipients are located overseas;

(e) how and where the School stores the information;

(f) how the School protects the personal information (including physical and technical measures);

(g) the School's practices relating to direct marketing, and promotion of the School (where those activities involve the use of personal information);

(h) what the School's practices are for deleting personal information when it is no longer needed;

(i) what procedures the School has in place to deal with requests by individuals to access or correct their personal information, or privacy complaints;

(j) any risk areas (e.g., where there is collection and use of sensitive information or ID documents, or where collection, use or disclosure of personal information might not be expected by the individual); and

(k) what changes may need to be made to comply with the APPs and reduce privacy risks.

3.4 Privacy documentation:

(a) review Privacy Policy and ensure the current version is available on the School's website. The Privacy Policy must be clearly expressed and up-to-date. It should be reviewed against the results of the internal review;

(b) review the School's privacy collection notices/statements to ensure they are clearly expressed and up-to-date and to identify where new collection notices/statements are needed. They should be reviewed against the results of the internal review;

(c) review any other relevant documentation as necessary (e.g., forms through which personal information is collected).

3.5 Consents:

(a) review existing consent processes to ensure they enable individuals to provide informed, specific and voluntary consent; and

(b) where the internal review identifies that consents are needed, ensure mechanisms exist or are implemented to obtain such consents.

3.6 **Practices, procedures and systems:**

Ensure practices, procedures and systems are in place that:

(a) will ensure the School complies with the APPs, including identifying and managing privacy risks and compliance issues; and

*If a school is part of a Diocesan system of schools it is likely that a large number of these functions will be carried out by the Diocesan office.

(b) will enable the School to deal with inquiries or complaints from individuals about its compliance with the APPs.

In addition to other steps referred to in this Section, this may include:

(c) reviewing the School's practices for responding to requests to access personal information (including by third parties), requests to correct personal information and privacy complaints;

(d) considering whether such practices should be documented, if not already (this is recommended); and

(e) conducting staff training (at least yearly).

3.7 Data breach response:

(a) review the School's data breach response plan to ensure it is up-to-date and reflects current roles and responsibilities, and the School's external legal and other advisor who could assist in the event of a breach; and

(b) run a short simulation of the data breach response plan as part of staff training.

3.8 **Security:**

Take steps to ensure personal information is secured in both hard copy and electronically. In particular, ensure that IT systems are appropriate to prevent unauthorised access and use. The Australian Cyber Security Centre has a tool that Schools can use to access their cyber security: https://www.cyber.gov.au/acsc/small-and-medium-businesses/cyber-security-assessment-tool. See also the *OAIC's Guide to securing personal information* https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information.

3.9 **Contractors:**

Before engaging service providers to handle personal information on the School's behalf, conduct appropriate due diligence and impose appropriate contractual obligations on the service provider. What is 'appropriate' will depend on the type and amount of personal information the service provider will handle.

3.10 **Overseas disclosures:**

If personal information is disclosed to recipients overseas, take steps to comply with APP 8. For example, ensure the contract with the overseas recipient requires the recipient to comply with the APPs when handling the personal information.

3.11 **Deletion:**

Consider whether the School should develop a protocol or similar for when certain types of personal information should be deleted (noting that in many situations, Schools have legal obligations to retain personal information).

3.12 **PIA:**

Consider whether a privacy impact assessment should be conducted when the School proposes to collect, use, store or disclose personal information in a way that is substantially different to current practices. For example, where a new information management system will be implemented.

3.13 Continuing obligations:

(a) ensure on-going compliance (e.g., regular review of information handling practices, conduct further audits where necessary, update Privacy Policy and collection notices, and repeat the other steps above at appropriate intervals or where an incident suggests a step should be repeated immediately); and

(b) ensure compliance with other applicable legislation, including health records legislation (see Section 2 of Part C of this Manual).

(c) keep IT procedures and other security measures under review.

Note: This is a summary only and NOT a full statement of obligations.

4. INFORMATION COVERED BY THE PRIVACY ACT

Types of information covered

The following types of information are covered by the Privacy Act:

(a) personal information;

(b) sensitive information; and

(c) health information.

What is 'personal information'?

4.1 Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information is true or not, and whether the information is recorded by the School in any material form or not. It includes all personal information regardless of its source.

4.2 In other words, if the information or opinion identifies an individual or allows an individual to be identified (including when connected with other information held by or reasonably available to the School) it will be 'personal information' within the meaning of the Privacy Act. It can range from very detailed information, such as medical records, to LGBTQI status (lesbian, gay, bisexual, transgender, questioning or queer intersex) and to other less obvious types of identifying information, such as an email address.

4.3 Personal information does not include information that has been de-identified so that the individual is no longer identifiable either from the information or from the information when combined with other information reasonably available to the School. Examples of de-identification techniques include removing identifiers, using pseudonyms and using aggregated data. Where practicable, Schools should use and share de-identified information, rather than personal information.

4.4 The APPs broadly apply to the collection and handling of personal information that is held in a School record. What constitutes a 'record' is broad and considered at Paragraphs 4.5 - 4.7 of this Part A.

What is 'sensitive information'?

Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. It also includes health information and biometric information.

What is 'health information'?

Health information is a subset of sensitive information. It is any information or opinion about the health (including illness, disability or injury) of an individual, the individual's expressed wishes about the future provision of health services, or a health service provided, or to be provided, to an individual. Health information also includes personal information collected in the course of providing a health service. For more details on the regulation of health information, see Section 2 of Part C.

What is a 'record'?

4.5 The Privacy Act regulates personal information contained in a 'record'. A 'record' includes a 'document' or an 'electronic or other device'. The definition is inclusive and therefore covers a wide variety of material which might constitute a record.

4.6 A 'document' is defined to include anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs.

4.7 There are some items which are excluded from the definition of 'record'. The exclusions relevant to a School are:

(a) a generally available publication; and

(b) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

Which acts and practices are exempt?

4.8 The Privacy Act does exempt certain acts and practices by APP Entities from the scope of the Privacy Act.

4.9 The following is a summary only of some key exemptions that may be of relevance to a School:

4.10 Small Business

A School with an annual turnover of $3 million or less will be deemed to be a 'small business' and will, subject to any exceptions, be exempt from the operation of the Privacy Act. The main exception relevant to Schools is where the School both holds health information (other than in an employee record) and provides a health service. In such a case, the School will not be considered to be a 'small business'.

NB: All schools should consider adopting the APPs as a matter of good practice even if deemed to be a small business.

4.11 Employee Records

Certain acts or practices directly relating to employee records are exempt from the scope of the Privacy Act. See Section 14 of Part C for more information on the employee records exemption.

5. EXAMPLES OF INFORMATION COLLECTED AND HELD BY SCHOOLS

Personal information likely to be collected

5.1 Some of the kinds of personal information likely to be collected and held in a 'record' (see Paragraph 4.2 of Part A) are set out below. These are examples only. Each School should assess whether the personal information it collects is reasonably necessary for its functions or activities (if not, it should not be collected).

5.2 For students this could include:

name, address, phone number, date of birth (and age), birth certificate, conduct reports, next of kin details, emergency contact numbers, names of doctors, school reports, assessments, referrals (e.g., government welfare agencies/ departments), correspondence with parents, photos, current/previous school, health fund details and Medicare number.[1]

5.3 For parents this could include:

name, address, email address, phone number, date of birth, vehicle registration details, occupation, marital status/problems, custody details, doctor's name and contact information, other children's details, donation history, maiden name of ex-students, alumni year, whether alumni had further education, professional experience and personal news.

5.4 For job applicants, staff members and contractors this could include:

name, company name and ABN, phone number, email address, tax file number (TFN), date of birth and age, contact details of next of kin, emergency contact numbers, including doctor, residency status/work visa status, qualifications, education, academic transcript, work permit, passport, details of previous salary, bank account number, superannuation details, marital status, letters of appointment/ complaint/ warning/ resignation, record of interview, leave applications, discipline issues, professional development appraisals, performance review, photograph, applications for promotions, references, commencement date, employment agency details, former employers, teacher registration number, blue cards, registration cards and the like.

5.5 Personal information might also be collected from other people such as board members, committee members, volunteers, neighbours, donors and others.

Sensitive information likely to be collected

5.6 The kinds of sensitive information that may be collected and held by Schools include:

(a) For students - religion, biometric templates, birth certificate, second language spoken at home, religious records, whether Aboriginal or Torres Strait Islander, nationality, country of birth, Sacrament/Parish (current Parish, name of referring Priest, date and place of Baptism, Confirmation, Eucharist and Reconciliation), and Baptism Certificate.

(b) For Parents - religion, country of birth, nationality.

(c) For job applicants, staff members and contractors - place of birth, religion, religious education, criminal record check, relevant child protection law information, member of professional associations, trade union membership, country of birth and nationality.

[1] Medicare numbers must only be collected if necessary and for limited purposes and are subject to specific rules regarding their use and disclosure in APP 9. If a School is unsure if it is permitted to collect Medicare numbers, legal advice should be sought. In addition, Medicare numbers are a type of 'sensitive information'. Schools should ensure that they give Medicare numbers the same level of security and protection as other types of sensitive information.

5.7 The following types of health information are likely to be collected and held by Schools.

(a) For students - medical background, immunisation records, medical records, medical treatments, accident reports, absentee notes, medical certificates, height and weight, nutrition and dietary requirements, assessment results for vision, hearing and speech, reports of physical disabilities, illnesses, operations, paediatric medical, psychological, psychiatric and psychometric information, developmental history, diagnosis of disorders, learning details (recipient of special procedures, assessment for speech, occupational, hearing, sight, ADD, Educational Cognitive (IQ)).

(b) For parents - history of genetic and familial disorders (including learning disabilities), miscellaneous health information contained in a doctor or hospital report.

(c) For job applicants, staff members and contractors - medical condition affecting ability to perform work (or e.g., use the School's fitness facilities), health information, compensation claims and doctor's certificates.

PART B

Responding to data breaches

1. Data Breaches

1. DATA BREACHES

Introduction

1.1 A data breach concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure (**Data Breach**).

1.2 Data Breaches are not limited to the malicious acts of third parties, such as theft or 'hacking', but may also arise from human error, a systems failure, or a failure to follow information handling or data security policies resulting in accidental loss, access or disclosure. Data Breaches are different from an interference with privacy that involves a breach of another privacy principle such as a failure to ensure personal information is accurate, up-to-date, complete and relevant under APP10 (see Section 8 of Part D – Data quality). The following are examples of when a Data Breach may occur:

(a) loss of smartphone or other School device or equipment containing personal information;

(b) cyber-attacks on the School's system, resulting in unknown third parties accessing or stealing personal information;

(c) accidental transmission of personal information such as student's reports to unintended recipients via e-mail; and

(d) loss or theft of hard copy documents.

1.3 All Schools are required to report certain data breaches under the notifiable data breaches scheme in Part IIIC of the Privacy Act (**NDB Scheme**).

1.4 A Data Breach is an 'eligible data breach' (**EDB**) if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach. Not all Data Breaches will be EDBs. For example, if a School acts quickly to remediate a Data Breach, and as a result of this action the Data Breach is not likely to result in serious harm, there is no obligation to notify any individuals or the OAIC. However, in some cases, a School may decide to voluntarily notify individuals and/or the OAIC. There are also limited exceptions to notifying affected individuals and the OAIC of an EDB in certain circumstances.

1.5 This Part provides guidance for Schools regarding:

(a) containing a Data Breach;

(b) assessing whether a Data Breach is an EDB and taking remedial action to reduce the likelihood of harm to individuals affected by the Data Breach;

(c) notifying the OAIC of an EDB and notifying individuals affected by an EDB, and potential exceptions to notification; and

(d) reviewing the Data Breach/EDB to prevent its reoccurrence in the future.

1.6 At the Annexures to this Manual the following tables have been included:

(a) Annexure 1. Summary of Mandatory Notification Procedures

(b) Annexure 2. Template Data Breach Response Plan

(c) Annexure 3. Data Breach Risk Assessment Factors

1.7 The OAIC's *NDB Scheme: Resources for agencies and organisations* are available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme (**OAIC Resources**).

Containing the Data Breach

1.8 Once a School suspects a Data Breach may have occurred, immediate steps should be taken to identify the Data Breach and if a Data Breach has occurred, to contain and limit it and this may involve stopping the unauthorised disclosure, shutting down the system that was breached, retrieving personal information, or changing computer access privileges or addressing security weaknesses.

Assessing whether the Data Breach is an EDB

1.9 Schools also need to determine whether the Data Breach is an EDB. This involves assessing whether:

(a) there has been a Data Breach – that is, whether there has been unauthorised access to or unauthorised disclosure of personal

information, or a loss of personal information in circumstances where the loss is likely to result in unauthorised access or disclosure; and

(b) if so, the Data Breach is likely to result in serious harm to any of the individuals whose personal information was involved; and

(c) remedial action is possible (so that serious harm is not likely).

1.10 1.Timing of assessment

(a) If Schools suspect an EDB may have occurred, they must conduct this assessment expeditiously, and take all reasonable steps to ensure it is completed within 30 days after the suspicion arises that a Data Breach has occurred. See sample data breach response plan set out in Annexure 2.

1.11 Is serious harm likely?

(a) Determining whether serious harm is likely is a threshold test and involves considering whether a reasonable person in the School's position would conclude that the Data Breach would be likely (more probable than not) to result in serious harm to any of the individuals to whom the information relates.

(b) This reasonable person test is aimed at ensuring only EDBs are reported to the OAIC – not every Data Breach. EDBs will be Data Breaches:

(i) that a reasonable person in the School's position (rather than the individual to whom the information relates or any other person) would conclude,

(ii) based on all of the information either immediately available to them, or available following reasonable inquiries or an assessment of the data breach,

(iii) that the unauthorised access to or disclosure of the particular personal information or personal information relating to the particular individual, is likely to result in serious harm to them.

(c) This test is designed to support the objective of the Privacy Act to promote the protection of the privacy of individuals while balancing the interests of entities carrying out their legitimate functions or activities. It also helps avoid unnecessary administrative burdens (both on entities such as Schools, and on the OAIC receiving notification), and 'notification fatigue' on the part of individuals.

1.12 What is serious harm?

(a) Serious harm is not defined in the Privacy Act, however in the context of a Data Breach, the OAIC Resources note that serious harm may include serious physical, psychological, emotional, financial or reputational harm. The Privacy Act (Section 26 WG) also sets out a non-exhaustive list of 'relevant matters' that may assist Schools in assessing the likelihood of serious harm. These include:

(i) the kind or kinds of personal information involved;

(ii) the sensitivity of that information;

(iii) whether the information is protected by one or more security measures and the likelihood any such security measures would be overcome, including the use of an encryption key to circumvent the encryption technology or methodology;

(iv) the person, or the kinds of persons, who have obtained, or who could obtain, the information;

(v) the likelihood that the person who has obtained the information, or has or could obtain, the information or knowledge required to circumvent the security technology or methodology;

(vi) the nature of the harm; and

(vii) any other relevant matters.

(b) Each factor is explored in more detail in Annexure 3

Example:

A teacher leaves a class list on the bus. The class list only contains names of students in the teacher's Year 11 class and no other details. The teacher informs the Principal. The Principal instructs the teacher to contact the bus company to try and recover the list but it cannot be found. The school tells the students what has happened but takes no further action.

Given that the personal information disclosed only consisted of the names of students, the kind of information indicates that serious harm was not likely to occur and the school's actions were appropriate.

Example:

A school sends an email to all parents in Year 7 about the sporting calendar for the term. Unfortunately, the wrong document is attached and all parents were sent a Risk Assessment for one of the students who had severe behavioural problems arising out of the students autism. The school became aware of this when a parent called them. The school recognised that this may be damaging to both the parents of the student identified and the student identified, given the vulnerability of this family. The school immediately sent an email to the Year 7 parents asking them not to open the attachment, to delete the email, and not to divulge the contents of the attachment if they had read it.

The school wrote to the parents of the student identified notifying them of what had occurred and what steps they were taking to prevent a reoccurrence in the future. As there was a risk of serious harm due to the wide distribution of the information, the sensitivity of the information, and the vulnerability of the family, the OAIC was also notified.

1.13 Can serious harm be prevented with remedial action?

(a) As part of assessing the likelihood of serious harm, Schools should take steps to consider whether remedial action to reduce any potential harm to individuals is possible (to prevent serious harm). The NDB Scheme provides that if entities take remedial action to prevent serious harm resulting from the Data Breach, then it will not be a Data Breach that must be notified. The School will need to assess whether the effect of the remedial action it takes would mean that the Data Breach would not be likely to result in serious harm to any of the individuals to whom the affected information relates. This may include action taken in relation to:

(i) the access or disclosure that has occurred before the access or disclosure results in serious harm to any of the individuals to whom the information relates; or

(ii) the loss of information before there is unauthorised access to or disclosure of the information so that there is no unauthorised access or unauthorised disclosure.

the loss of information *after* there is an unauthorised access to or disclosure but *before* the access or disclosure results in serious harm to any of the individuals to whom the information relates.

Example:

A school counsellor leaves their smartphone on public transport while on their way to work. The smartphone provides access to the school counsellor's work emails that contain the names of students and notes from counselling sessions with students at the school. When the school counsellor arrives at school they realise that their smartphone has been lost, and ask the school IT support staff to remotely delete the information on the smartphone.

Due to the security measures on the smartphone, the school IT support staff are confident that its contents have been wiped and that the personal information on the smartphone was not accessed by anyone in the short period between the loss of the smartphone and when its contents were deleted.

Example:

A school finds that an ex-employee of We Assist Pty Ltd, which has been contracted to conduct a fundraising campaign for a new building at the school, has taken a list of the names and addresses of the contributors to the fund and the amount they donated. The ex-employee has been using this database with his new employer NewCo Pty Ltd, also a fundraising company. The school immediately contacted We Assist and demanded that it take immediate action to recover the database used by NewCo, and seek an undertaking from NewCo that the database would be destroyed. It also wrote to each donor advising them what had happened. We Assist received the undertaking demanded and passed it onto the school.

As the database had been destroyed by NewCo, the school did not inform the OAIC as it had taken action before the disclosure resulted in serious harm and had required We Assist to obtain confidentiality undertakings from its employees to emphasise the need for confidentiality.

1.14 What if multiple organisations are involved in the EDB or suspected EDB?

(a) If a School or other organisation (e.g., a cloud service provider or other third party supplier) are together involved in a Data Breach affecting personal information of individuals the School handles (i.e., both the School and the other organisation 'hold' the information), and either the School or other organisation has made an assessment about the suspected Data breach to determine whether there has been an EDB, the School or other organisation involved in the Data Breach is not required to undertake the same assessment and may rely on the assessment already made. Despite this, in some cases Schools may also want to undertake their own assessment or may have information that would help determine whether serious harm is likely to any individual.

Example:

A school implements a cashless canteen system Healthy Bites to allow students and their parents to order recess and lunch online. The system allows parents to view what their child purchased at the canteen and to top up their account using their credit card details. The Healthy Bites portal is hosted by Healthy Bites Pty Ltd, and is not hosted by the school. As part of the new system the school provided an Excel export from their information system to Healthy Bites, providing the student number of each student plus the names of all students and their parents to the company. Sometime later the school Principal is advised that the Health Bites portal has been hacked and the information of students and parents may have been accessed inappropriately. The school is aware that parents conduct credit card transactions in the system. Healthy Bites informs the school that they have assessed the risk of serious harm and have concluded that the Data Breach is unlikely to result in serious harm to students or parents. They also informed the school that as the system is hosted by Healthy Bites and not the school, it is not the schools responsibility to report this Data Breach to the parents involved or the OAIC. The terms of the contract between the school and Healthy Bites is silent on who should take responsibility for assessing a Data Breach, and notifying individuals and the OAIC if it is an EDB.

The school took the view that as the information accessed came from the school and the use was for an activity associated with the school, it did have a responsibility in relation to the security of the information. The school decides that there is a risk of serious harm to parents and some students and on that basis decides it is an EDB and, notifies parents whose information was involved and the OAIC.

Notifying individuals and the OAIC

1.15 Once a School is aware that there are reasonable grounds to believe there has been an EDB, the School must, as soon as practicable:

(a) make a decision about which individuals to notify;

(b) prepare a statement for the OAIC in accordance with the OAIC *Notifiable Data Breach statement – Form* – this can be emailed or lodged online via the OAIC website (https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach); and

(c) notify individuals of the contents of this statement as soon as practicable after notifying the OAIC.

1.16 The School will still need to be continuing to take what steps it can to contain the Data Breach and minimise the likely harm as well as deciding what steps it would recommend the individuals can take to protect themselves as it will need to explain this in the statement it must give to the OAIC and individuals, as explained below.

1.17 The NDB Scheme provides three options for notifying affected individuals of the statement provided to the OAIC:

(a) Option 1: notify all individuals whose personal information was part of the EDB;

(b) Option 2: notify only those individuals at risk of serious harm from the EDB; or

(c) Option 3: if neither option 1 or 2 are practicable, the School must publish a copy of the statement provided to the OAIC on its website if it has one and take reasonable steps to publicise the contents of the statement.

1.18 A School can use any reasonable method to notify individuals via option 1 or 2 (e.g., telephone call, SMS, physical mail, or in-person conversation), or their usual method of communicating with that individual.

1.19 Where the individual being notified is a student, it may be appropriate to notify the parent or guardian instead of or as well as the student. The age and maturity of the student will be an important factor when considering who to notify. This issue is discussed more fully in relation to consent and young people in Section 7 of Part C.

1.20 Schools can tailor the notification to individuals, as long as it includes the content of the statement Schools must provide to the OAIC. The NDB Scheme requires the statement and the notification to individuals to include:

(a) the identity and contact details of the School;

(b) a description of the EDB and the organisation (e.g., the School) that has reasonable grounds to believe the EDB has happened;

(c) the particular kind, or kinds, or information concerned;

(d) recommendations about the steps that individuals should take in response to the EDB.

1.21 In addition, if the EDB involves two entities, the statement may also set out the identity and contact details of those other entities.

1.22 There are limited relevant exceptions to Schools' obligations to notify the OAIC and/or individuals. These are

(a) if the EDB affects the security of personal information held by both the School and other organisations, only one organisation needs to prepare the statement and give notification of the EDB, for all affected organisations to comply with the notification requirements under the NDB Scheme. In such circumstances, the notification should set out the identity and contact details of both entities; and

(b) where the OAIC makes a declaration that an entity is not required to comply with the notification requirements under the NDB Scheme or can delay giving notice. This declaration can be made as a result of a submission by the School about reasons why notification to OAIC or some or all of the individuals should not be made or delayed.

1.23 Whilst not mandatory under the NDB Scheme, in some circumstances it may be appropriate to also notify third parties such as:

(a) Police or law enforcement – if theft of other crime is suspected – it can be an offence not to notify an indictable offence to the police;

(b) Credit card companies or financial institutions – e.g., if the School or a service providers have obligations under other regulatory schemes such as credit card payment processors who are subject to the Payment Card Industry Security Standards or their assistance is necessary for contacting individuals or mitigating harm;

(c) other internal or external parties not already notified – if they may be impacted by the EDB (e.g., professional bodies, or the ATO if Tax File Numbers are affected); and

(d) ReportCyber https://www.cyber.gov.au/acsc/report (part of the Australian Cyber Security Centre)– if the School has been a victim of cyber-crime. They can offer further advice and support in relation to cyber security incidents and a report can be lodged and followed up by the appropriate agency.

Reviewing the Data Breach/EDB

1.24 Whether the incident that occurs is a Data Breach or an EDB that requires notification under the NDB Scheme, conducting a follow up review of the Data Breach once the above steps have been taken is very important so that Schools take action to prevent future breaches and ensure ongoing compliance with their data security obligations and overarching obligation to manage the personal information they hold in a compliant manner. This includes:

(a) investigating and understanding the cause(s) of the Data Breach or EDB;

(b) developing a prevention plan and conducting audits to ensure the plan is implemented;

(c) considering changes to policies and procedures; and

(d) further training staff.

Consequences

1.25 The NDB Scheme is subject to the existing regulatory and enforcement framework overseen by the OAIC as set out in the Privacy Act. This means that the consequences of a School breaching a requirement of the NDB Scheme, include:

(a) an investigation by the OAIC into the causes of the Data Breach/EDB and the School's response;

(b) a determination by the OAIC that the School take specified steps to remedy noncompliance, perform any reasonable act to redress any loss suffered, pay monetary compensation or publish a statement about the breach;

(c) a request that the School provide an enforceable undertaking that it will take, or refrain from taking, specified action. In the case of serious or repeated noncompliance; or

(d) an application by the OAIC to court to impose a civil pecuniary penalty of up to the greater of $50 million or 30 percent of the School's adjusted turnover in the relevant period.

1.26 The OAIC also has powers to obtain information or documents relating to Data Breaches and EDBs.

Voluntary notification

1.27 Even when the Data Breach is not an EDB under the NDB Scheme, there may be instances where a School considers it necessary to voluntarily notify one or some affected individuals and/or the OAIC of a Data Breach, in accordance with its obligations under APP11 to take reasonable steps to keep the personal information it holds secure (see Section 9 of Part D) as well as for managing the reputational impact to the School and complying with its duty of care obligations.

Example:

A school provides all students and staff with access to the cloud based system, Google Docs. Students and staff access this system using the school username and password. The Head of Year Nine sets up a Google Sheet (similar to Excel) to track students in Year Nine who attend learning support classes to further develop their literacy skills. The sheet lists the students' names, particular areas of learning need: grammar, spelling, reading and anecdotal notes about each student's progress. The Google sheet is shared with all teachers who teach these students so they can remain aware of their progress. The settings are set to 'Public on the web – anyone on the Internet can find and access'. Subsequently the school is contacted by a parent of one of the students listed on the sheet to inform them that the sheet is publicly available on the web. The school is able to establish that the sheet has only been accessed by teachers and the parent who contacted the school. The school also immediately rectifies the situation by changing the sharing settings of the sheet to 'Off – Specific People', informs the parent of the action taken, undertakes an audit of all school IT systems and requires all school staff to take part in privacy training.

The school does not otherwise notify parents, students or the OAIC as the data breach did not result in serious harm to the student.


False
True
False
RROR_Z":
False
False
True
end -add back the deselected mirror modifier object
cts.active = modifier_ob
(modifier_ob)) # modifier ob is the active ob
= 0

PART C

Particular issues for Schools

1. Privacy Policies and Collection Notices

Privacy Policy (APP 1.3-1.6)

How to comply

Training staff

Ensuring individuals are fully aware of collection (APP 5.1).

Comment

How to comply

NAPLAN Notices

2. Health Information

What is health information?

Collection of health information

Use or disclosure of health information

Health information and employees

Additional requirements in States and Territories

Inconsistencies between Federal and State laws

3. Sharing of Photographs and Videos

Introduction

Summary

When is consent not required?

When and how should general and specific consent be sought

Other considerations for consent

Other matters

4. Counselling Records

General

School Counsellors generally

Professional Associations

Effect of employment status of Counsellors

Disclosure of reports

Duty of Care

5. Access to Records by Students and Parents

Background

Timing of response

When can parents access their child's personal information?

When can a parent access the personal information of another child related to their child?

Denying access on the basis of an unreasonable impact on the privacy of others.

Denying access on the basis of legal professional privilege

Denying access on the basis of existing or anticipated legal proceedings

Denying access on the basis that it would reveal commercially sensitive evaluative information

Access to health information

6. Digital Learning

Background.

Remote lessons

Digital collection, storage or sharing of materials associated with a classroom or lesson

School approved email and platforms

7. Consent and Young People

1. PRIVACY POLICIES AND COLLECTION NOTICES

Privacy Policy (APP 1.3-1.6)

1.1 Requirement:

A School must have a clearly expressed and up-to-date policy about the management of personal information by the School (APP 1.3).

1.2A Requirements:

The Privacy Policy of a School must contain the following information:

(a) the kinds of information it collects and holds;

(b) how it collects and holds information;

(c) the purposes for which it collects, holds, uses and discloses information;

(d) how an individual may access and seek correction of their information;

(e) how an individual may complain about a breach of the APPs and how the School will deal with that complaint; and

(f) whether the School is likely to disclose information overseas and, if so, the countries in which the recipients are likely to be located (if practicable to specify) (APP 1.4).

1.2B In addition, from 10 December 2026, the Privacy Policy of a School must contain specified information about the School's use of personal information as part of any automated decision making the School undertakes. This applies where:

(a) the School has arranged for a computer program to make, or do a thing that is substantially and directly related to making, a decision;

(b) the decision could reasonably be expected to significantly affect the rights or interests of an individual; and

(c) personal information about the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision.

1.3 Requirement:

A School must take such steps as are reasonable in the circumstances to make its Privacy Policy available free of charge, and in such form as is appropriate (APP 1.5). A School should make its Privacy Policy available on its website.

1.4 Requirement

If a person requests a copy of the Privacy Policy in a particular form, the School must take such steps as are reasonable in the circumstances to give the person or body a copy in that form. (APP 1.6)

1.5 In addition, it is important that policies relating to privacy are understood by staff and are adequately enforced.

How to comply

1.6 Adopt a Privacy Policy which expresses, in plain language, the School's policy or policies on its management of personal information. An 'up-to-date' Privacy Policy should be one that is a 'living document' and is reviewed regularly. It would be sensible to diarise a review at least once every 12 months. The APP Guidelines provide that, 'at a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in- house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity'.

1.7 The Privacy Policy (an example is at Annexure 5) should cover the following issues:

(a) the kinds of personal information the School collects and how it collects and uses this information;

(b) sharing and disclosing information (internally, to 'related Schools', to third parties);

(c) direct marketing;

(d) the transfer of information overseas;

(e) storage of information;

(f) access and correction of information;

(g) complaints; and

(h) if the School undertakes automated decision making using personal information (see paragraph 1.2B above), the kinds of personal information used and the kinds of decisions made.

1.8 The sample Privacy Policy at Annexure 5 is intended to comply with APP 1 and should be adapted as required by the School. Not only can this Privacy Policy be used to help inform individuals about the practices of the School in relation to personal information, but it can also serve as a guide to the School's staff as to the standard to be applied in respect of handling personal information and ensure consistency in the School's approach to information privacy.

1.9 Schools should make the Privacy Policy available on the School's website and draw attention to it when collecting personal information.

Training staff

1.10 The key to achieving compliance and ensuring continued compliance with the Privacy Act will be through the conduct of the School's employees and other staff members. Consequently, the School's staff members must be trained in the principal requirements of the Privacy Act.

1.11 There are a number of ways that employees and other staff members should be made aware of the requirements of APP 1 (and the other obligations under the Privacy Act). These include raising general awareness by:

(a) circulating the Privacy Policy to all staff and requiring them to acknowledge they have read it;

(b) informing staff of the requirements of confidentiality and extending this obligation contractually where necessary; and

(c) holding internal seminars and workshops.

1.12 As part of the training staff should be reminded that a large proportion of data breaches arise from human error. Often this error is sending a document to the wrong recipient.

Ensuring individuals are fully aware of collection (APP 5.1)

1.13 Requirements:

At or before the time (or, if not practicable, as soon as practicable after) a School collects personal information about an individual, the School must take such steps (if any) as are reasonable in the circumstances to notify or make the individual aware of such of the following matters that are reasonable in the circumstances:

(a) the School's identity and contact details;

(b) if the individual may not be aware that the information has been collected or if the School collected the information from a third party, the fact that it has been collected and the circumstances of the collection;

(c) if collected under or authorised by law, the fact that the collection is so

required or authorised (including details of the law requiring or authorising collection);

(d) the purposes for which it is collected;

(e) the main consequences if it is not collected;

(f) any other entities or types of entities to whom the information may be disclosed;

(g) that the Privacy Policy contains information about how an individual can access and seek correction of information;

(h) that the Privacy Policy sets out how an individual may complain about a breach of their privacy and how the complaint may be dealt with; and

(i) whether information is likely to be disclosed overseas and, if so, to which countries, if practicable to specify.

Comment

1.14 Deciding on whether a School should make individuals aware of the required matters 'at or before the time of collection' will depend on the circumstances. This can be done after collection of the information if there are practical problems in doing so before collection.

1.15 APP 5.1 has a 'double reasonableness' provision. A School is only required to take 'reasonable steps' to inform people of such of the required matters that are 'reasonable' in the circumstances. Therefore, it is recognised that where such of those matters are obvious, irrelevant or can be easily located (e.g., the identity of the School) it may not be necessary to inform people of that matter in a collection statement. The APP Guidelines provide that it is the responsibility of the entity to be able to justify not taking any steps.

1.16 In the same way, where the circumstances of collection make a matter listed in APP 5.1 obvious, then the 'reasonable steps' might not involve any active measures because the circumstances speak for themselves. For example, if the matters contained in APP 5.1 were made available to an individual for a certain type of collection, then the same collection later may not require that the APP 5.1 matters (if unchanged) be repeated to the individual.

1.17 Deciding what are reasonable steps and what are matters which are reasonable to include involves balancing a number of possible factors, including the importance to the individual of having the relevant knowledge and the time and cost to the School in providing that information (however, a School is not excused from taking steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so).

1.18 The description of the purposes of collection can be reasonably general as long as the description is adequate to ensure that the individual is aware of what is going to be done with their personal information. Internal purposes that form part of normal business practices, such as auditing, business planning or billing do not have to be described.

1.19 Taking 'reasonable steps' to inform an individual about usual disclosures would ordinarily mean either giving general descriptions of sets of people and entities to whom the information may be disclosed (for example, State Government educational authorities and other schools) or listing each member of the set.

1.20 A School does not need to mention disclosures that the APPs permit, but in practice happen only rarely (e.g., a disclosure to Police or child protection authorities where required by law).

1.21 Reasonable steps must be taken to tell the individual about any law that requires the individual to provide, or the School to collect, personal information in the particular situation. In describing the law, the School need not specify the exact piece of legislation (although it would be desirable to do this where possible). A statement like 'The New South Wales Education Act requires us to collect this' would ordinarily be adequate.

1.22 A School need not describe all possible consequences of not providing personal information. Only significant (and non-obvious) consequences would need to be described.

1.23 A School is required to describe the fact that it collects personal information and the circumstances of that collection. However, this is only required when the School collects the personal information from someone other than the individual or the individual may not be aware that the School has collected the personal information. If the School collects the information directly from the individual, and the individual is aware of this collection, the School is not required to describe the fact and circumstances of collection.

How to comply

1.24 A common sense and pragmatic approach should be taken by the School when complying with APP 5.1 and APP 5.2.

1.25 Annexure 5 contains example privacy collection notices that should be adapted as required by the School. This includes a 'standard collection notice' (for parents and students), an employment collection notice (for job applicants) and a contractor/volunteer collection notice.

1.26 The APPs make it clear that there will be occasions where it is reasonable not to advise people of some or all of the matters set out in APP 5.2. This would be the case, for example, when those matters are obvious or likely to be known.

1.27 As the information a School requires varies over the period of a student's enrolment, it is suggested that the 'standard collection notice' (see Paragraph 3.45 of Part D) be reviewed and updated each year.

1.28 Where the School collects personal information about those who have not seen any collection notices (e.g., third parties) or where the collection notices do not cover a particular situation, then the School should consider, with reference to the APPs and any available Guidelines, whether it needs to take additional steps to comply with APP 5.1 and notify those people of the matters set out in APP 5.2. In particular, where a School intends to use a film including a student or a student's photo in a public forum (such as on television or on social media, such as Facebook and Flickr) the student's and/or the student's parents' permission should be sought as appropriate. This is

further considered in Section 3 of Part D of this Manual.

1.29 The 'standard collection notice', which is drafted to cover the School's usual collection practices, could be tailored to suit specific situations and should deal with the matters listed in APP 5.1 concerning how any personal and sensitive information collected from the individual about him/herself or a third party would be dealt with.

1.30 The 'standard collection notice' should be reproduced in enrolment forms (and at any other initial points of collection) and could also be placed in each student's School diary. It is suggested that the then-current notice be sent at the commencement of each school year to parents of students at the same time as other materials are sent.

1.31 The School should consider placing a collection notice in other relevant documents (e.g., it may be appropriate to insert a collection notice in a form designed to collect a student's medical information).

NAPLAN Notices

1.32 All schools in Australia are required to participate in the National Assessment Program – Literary and Numeracy (NAPLAN). The sample standard collection notice in Annexure 6 (as well as the example privacy policy in Annexure 5) include information that reflects the personal information flows associated with NAPLAN (including the potential disclosure by Schools of parents' and students' personal information as part of NAPLAN online).

1.33 Schools will also be provided with a separate NAPLAN specific notice that Schools will need to provide to parents. This notice will need to be provided to parents each year before NAPLAN testing commences (usually as part of an information pack with general information about NAPLAN). This NAPLAN specific notice is not included this Manual.

2. HEALTH INFORMATION

2.1 Health information enjoys special protection under the Privacy Act and under the following State and Territory legislation:

(a) Health Records and Information Privacy Act 2002 (NSW);

(b) Health Records Act 2001 (Vic); and

(c) Health Records (Privacy and Access) Act 1997 (ACT).

Schools collect substantial amounts of health information about students and staff and, on occasions, parents. They need to take particular care in collecting, using and disclosing health information.

What is health information?

2.2 Under the Privacy Act, '*health information*' includes, amongst other things, information or an opinion about:

(a) the health, disability or injury of an individual;

(b) an individual's wishes about the future provision of health services to the individual; and

(c) a health service provided, or to be provided, to an individual.

2.3 It also includes all personal information (regardless of whether it would otherwise be health information) collected to provide, or in providing, a health service to an individual.

2.4 The Privacy Act provides that a '*health service*' includes an activity performed to assess, record, maintain or improve an individual's health, to diagnose an illness or disability, or to treat an individual. Legislation in some States and Territories specifically includes '*mental and psychological*' health as being health information. Schools should treat health information as including information about an individual's mental and psychological health. A report from a school counsellor or a consultant psychologist will, therefore, often contain health information. For more information on school counsellors see Section 4 of Part C.

2.5 Accordingly, a School may provide a 'health service' in circumstances including where it engages:

(a) a school nurse;

(b) a school counsellor;

(c) a school psychologist; or

(d) a sports physiotherapist,

who assesses, records, maintains or improves a student's health, diagnoses a student's illness or disability, or treats a student. All personal information that a school collects to provide that health service, must be treated as health information. The provisions are not intended to apply where, for example, a member of School staff carries out emergency first aid on a student (although the provisions will apply to health information in any record the School makes of the emergency first aid carried out on the student). Schools sometimes employ professionals to supply health services and sometimes, in effect, provide such services through their regular teaching staff.

2.6 If a School is unsure if a service it provides is a 'health service', it should treat all the personal information it collects in providing that service as health information.

2.7 Even where a School does not provide a health service, the School will need to ensure it complies with the higher level of protection under the laws when it collects, uses and discloses health information.

2.8 The key requirements that apply to the handling of health information are set out below.

Collection of health information

2.9 Health information generally should only be collected:

(a) with the consent of the student or parent (depending on the student's age);

(b) where it is required to allow the School to exercise its duty of care or is otherwise required or authorised by law; or

(c) where it is necessary to lessen or prevent a serious threat to the life, health or safety of an individual and it is impracticable to obtain consent.

2.10 In most cases in Schools, the collection will be with the consent of the individual or, in the case of students, the consent of the parent. This is because it is provided by them either in answer to a question or to put the School on notice of a particular problem or to explain an absence. In some cases however, a School may wish to collect information from a third party, such as another School, in circumstances where it is necessary for the School to exercise its duty of care. This may occur for example where a School had some responsibility for a student with a disability or health problem from another School. In such a case it is likely the school disclosing the information would need the consent of the student or parents unless it is able to rely on a power given by statute, such as Chapter 16A of the *NSW Children and Young Persons (Care and Protection) Act.*

2.11 Where a School records an incident at school where a student suffers an injury, this will constitute collection of health information. This is required if the School is to exercise its duty of care.

Use or disclosure of health information

2.12 It is important to remember that health information, in particular, usually should only be used or disclosed:

(a) for the purpose for which it was collected or a **directly** related secondary purpose;

(b) to exercise the School's duty of care or as otherwise required or authorised by law; or

(c) to lessen or prevent a serious threat to the life, health or safety of an individual and where it is impracticable to obtain consent.

2.13 Health information of a student should not be disclosed to third parties, such as to another parent or an organisation or school which has temporary care of the student unless the School considers that it is reasonably necessary to disclose it to ensure that the health or safety of the student is maintained (in circumstances where it is not practicable to obtain consent or, in some cases, even where consent is refused).

2.14 In order to provide appropriate protection to health information it is also important that it be kept secure and only staff who have a need to know the information are given access to it.

2.15 If it is necessary to include the information in a notice to staff, care should be taken that the notice is not accessible by non-staff members.

2.16 Difficult issues may arise where a School becomes aware of health information about a student which the student does not wish to be disclosed to a parent or to both parents. If such a situation occurs it may be necessary to seek external expert advice as to how to address the issue.

Health information and employees

2.17 As will be discussed in Section 14 of this Part C, certain acts or practices directly relating to employee records are exempt from the scope of the Privacy Act. An employee record relates to the employment of an employee of the employer. Health information of an employee may sometimes be considered as part of an employee record where it directly relates to a current or former employment relationship between the employer and the individual.

2.18 Importantly, the employee records exemption does not apply to the collection of any health information about an employee, and Schools need to comply with the Privacy Act in relation to that collection.

2.19 In New South Wales, information about an individual (including health information) that forms part of an employee record within the meaning under the Privacy Act will not be covered by the *Health Records and Information Privacy Act 2002* (NSW) (in effect, there is an employee records exemption from the NSW Act). The same exemption is not contained within the *Health Records Act* 2001 (Vic) and *Health Records (Privacy and Access)* Act 1997 (ACT). In those jurisdictions, health information which is contained in an employee record will be covered by the provisions of that legislation.

Additional requirements in States and Territories

2.20 In New South Wales, the *Health Records and Information Privacy Act* 2002 (NSW) implements a privacy regime for health information held in the New South Wales public sector and the private sector (except small businesses as defined in the Privacy Act). The Act allows for individuals to obtain access to health information and establishes a framework for the resolution of complaints regarding the handling of health information. The Act contains 16 Health Privacy Principles that outline how health information must be collected, stored, used and disclosed. The Act applies to persons who have been deceased for a period of 30 years or less.

2.21 A child may not rely on any right or powers conferred under the Act if the child is incapable (despite the provision of reasonable assistance by another person) by reason of age of understanding the general nature and effect of, or communicating their intentions, with respect to that particular provision. In such cases, an authorised representative of a child, such as a parent or guardian, may act on their behalf.

2.22 In Victoria, the *Health Records Act 2001* (Vic) covers the handling of all health information held by health service providers in the state public sector and the private health sector. The Act contains 11 Health Privacy Principles adapted from the NPPs (the predecessor to the APPs). The Act applies to persons who have been deceased for a period of 30 years or less, as well as small business operators (and other organisations). As noted above, the Act also applies to information contained in employee records.

2.23 The Act provides that a complaint about a breach may be made by a child or on behalf of the child by a parent, any other person chosen by the child, or any other person who the Health Services Commissioner determines has a sufficient interest in the subject matter of the complaint. Additionally, a child may request access to or correction of health information only where they are capable of understanding the nature and effect or making such a request or communicating the request personally. Otherwise, an authorised (such as a parent or guardian) of the child may exercise the right to make that request.

2.24 In the ACT, the *Health Records (Privacy and Access)* Act 1997 (ACT) regulates the handling of health records held in the public sector in the Australian Capital Territory and also applies to acts or practices of the private sector. The Act contains 14 Privacy Principles that have been modified to suit the requirements of health records. The Act applies to deceased persons in the same way as they apply in relation to an individual who is not deceased. As noted above, the Act also applies to information contained in employee records.

2.25 Additionally, the ACT provides that a right or power conferred upon a child (a person who is under 12 years old) or a young person (a person who is 12 years old or older, but not yet 18 years of age) is exercisable only by a person with parental responsibly for the child or young person and is not exercisable by that child or young person on their own behalf. However, there are some exceptions. For example, a young person can exercise the right of access to a health record if the young person has sufficient maturity and developmental capacity to understand the nature of the young person's request to access and the nature of the record.

Inconsistencies between Federal and State laws

2.26 In addition to the Privacy Act, Schools in New South Wales, Victoria and the Australian Capital Territory who are recognised as providing a health service or who collect, store, use or disclose health information, will also be required to comply with the relevant health information legislation in those jurisdictions. Such Schools will therefore be required to comply with two sets of principles: the APPs in the Privacy Act and the relevant set of Health Privacy Principles or Privacy Principles.

2.27 While the principles in New South Wales, Victoria and the Australian Capital Territory legislation were based on the NPPs (the predecessor to the APPs), they are not identical, and in some cases impose different (including higher) standards. The scope of the State and Territory legislation may also differ from the

federal legislation. For example, the Victorian Act covers small business operators and employee records, unlike the Privacy Act. The information handling principles in the New South Wales, Victorian and Australian Capital Territory legislation also differ from each other, so that information passing from one jurisdiction to the other may become subject to a different set of rules. This is something Schools should bear in mind if they are transferring such information to other jurisdictions (each jurisdiction also has requirements that must be met before such cross-border transfers occur).

2.28 The Privacy Act expressly allows State and Territory privacy legislation to operate to the extent that such laws are not directly inconsistent with the Privacy Act. Insofar as the various Health Privacy Acts provide more stringent provisions than the Privacy Act but do not contradict it, Schools are required to comply with both sets of legislation.


Use
relevant
charts
and
graphs

3. SHARING OF PHOTOGRAPHS AND VIDEOS

Introduction

3.1 In most circumstances, photographs and footage of students, parents and other members of the School community, will be their personal information. Individuals are generally sensitive to photographs and footage of them being taken and published, particularly as technology gives greater opportunities for this information to be misused. Therefore, care must be taken by Schools when taking, using and sharing photographs and footage that include images of individuals.

3.2 When a School wishes to use footage or a photo that includes a student's (or other individual's) image, it must consider whether consent is required, particularly if any student (or their parent) was not aware that the footage or photo:

(a) could be used or published for a particular purpose; or

(b) could be published in a particular location such as on the School's website, television or on social media (for example on a public Facebook page as opposed to limited publication only available to students, parents and possibly alumni). This includes publishing the School newsletter, yearbook and similar publications in these locations.

Summary

3.3 Provided the Standard Collection Notice in Annexure 6 of this Manual is provided to students or their parents (as relevant), Schools can share photographs and footage of students with the school community (i.e., current, future and past students, parents and teachers) (**School Community**) for the purpose of reporting on school activities and events. This includes sharing via locations that are only accessible by the School Community (e.g., a closed School app).

3.4 For any other uses or discloses, the School should generally seek consent. It is recommended that Schools utilize:

(a) an annual general consent form (with separate tick boxes) that is completed at the beginning of each school year; and

(b) a specific consent form for particular situations which may not be covered by the general consent.

These two consent forms are explained further in Paragraph 3.12 of this Part C.

When is consent not required?

3.5 Provided students or their parents (as relevant) are provided with the Standard Collection Notice in Annexure 6 of this Manual, Schools do not need to seek consent to:

(a) include footage/photos relating to academic and sporting achievements, student activities and similar news in:

(i) the School's app it uses to communicate with parents and students (provided this is only accessible by parents, students and school staff);

(ii) the School newsletter, magazine and intranet, **provided** the School newsletter and magazine are only available to the School Community (e.g., they are not published on the School's public Facebook page); or

(b) distribute footage/photos of students in the School's concerts or plays to parents (this includes the sale of such footage/photos to parents).

This is explained below.

3.6 Consent is not required for a School to use (and disclose) footage or a photo where the School's use (or disclosure) is:

(a) related to the purpose for which the footage or photo was collected/ taken by the School; and

(b) reasonably expected by the student (or other individual who appears in the photograph/footage).

3.7 In relation to point 3.6(a) (related purpose), often it will not be difficult to show that the purpose for which a School wishes to use footage or a photo is related to the purpose for which the footage/photo was collected. For example, where a School takes a photo at a sporting event and includes the photo in the School newsletter to report to parents on the sporting event.

3.8 In relation to point 3.6(b) (reasonable expectation), the Standard Collection Notice at Annexure 6 of this Manual, provides as follows:

> *School activities and news (including student achievements) are frequently published in the School's journals, newsletters and magazines, on our [insert name of school app – assuming it is accessible by parents, students and teachers only], on our intranet or otherwise shared with the School community (current, future and past students, parents and teachers). This may include personal information (including photographs and videos) of students and parents involved in School activities such as academic and sporting events and achievements, concerts and plays, school camps and school excursions. The School will obtain permissions [annually] if we would like to include photographs or videos [or other identifying material] of students (or parents) in our promotional material or otherwise make this material available to the public such as on the internet.*

3.9 This creates a reasonable expectation that footage/photos relating to academic and sporting events and achievements, student activities (including concerts and plays, school camps and school excursions) and similar news may be included in the School newsletter, magazine and intranet, or otherwise shared with the School Community.

When and how should general and specific consent be sought

3.10 As a general rule, Schools should seek consent when they want to use footage or photos in a way different to that set out in Paragraph 3.5 of this Part C. For example, if the School would like to include such footage/photo in promotional material or make it available on the internet (such as the School's website or Facebook page available to the public).

3.11 Schools should carefully consider what consent to seek and how. To the extent that it is possible, Schools should seek specific time bound consent to use an student's image for a particular purpose and refrain from asking for 'bundled' consent which covers a number of uses as these are less likely to be valid consents. Where possible, consent forms should give students (parents) the option of choosing what uses to agree to.

3.12 It is recommended that Schools utilize:

(a) an annual general consent form (with separate tick boxes) that is completed at the beginning of each school year. An example is set out in Annexure 6[2]; and

(b) a specific consent form for particular situations which may not be covered by the general consent. This includes specific marketing campaigns, regardless of whether general consent for marketing has been obtained. For example, if a student photo will be on the side of a bus or an advertisement in a newspaper or a marketing brochure. This will ensure the consent is informed, current and specific.

3.13 Consent should generally be sought from older students and the student's parents and otherwise in accordance with the school's policy on obtaining consent. This issue is discussed more fully in relation to consent and young people in Section 7 of Part C of this Manual.

3.14 The following table compares how consent should be sought for different uses of footage and photographs. If a School is unsure if consent should be obtained, it should err on the side of caution and seek consent (which is specific to the particular intended use of the footage or photograph).

[2] The example form has been prepared from a privacy perspective only. It does not address any associated copyright issues and additional wording may need to be included (or an additional form used) to address such issues. Schools should obtain legal advice if they are unsure how to address any copyright issues.

Intended use of film/photograph	Consent
Use of footage/photos relating to academic and sporting achievements, student activities and similar news in the School newsletter, magazine and intranet (provided they are only available to the School Community)	No consent required (provided student/ parent has been provided with the Standard Collection Notice). In notifications about the event, include a short sentence informing students/parents that photos /videos will be taken and how they will be used/shared.
Internal uses (i.e., those where the parents can see the footage/photo, but not the general public) not covered by row 1.	Consider whether the use is related to the purpose for which the footage/photo was collected and reasonably expected by the student. If in doubt, seek a separate written consent for the particular use.
External use (e.g., School's website, public social media and television) where the student is not identified or not reasonably identifiable*	No consent needed as the student is not identifiable or reasonably identifiable.
External use where the student is identified or reasonably identifiable* e.g., School's website, public social media and television and sharing with third parties for specific distribution e.g., to news sites announcing student achievements.	Seek a separate written consent for the particular use. Depending on the circumstances, this may be covered by a general consent sought for photographs/footage to be published on e.g., public social media for promotional purposes (unless the photograph/video is of a parent – such as promoting a Mother's Day event on social media).

*'Reasonably identifiable' reflects the definition of 'personal information' in the *Privacy Act 1988* (Cth). In practical terms, consider if the individual is easily identifiable (e.g., if the student appears by themselves, or with only a small group of students). The fact that a student is not named will not, by itself, mean that they are not reasonably identifiable. A student may not be reasonably identifiable where they are in a large crowd of students (as opposed to a particular class of students that are identified as e.g., year 5, class B).

Other considerations for consent

3.15 The consent should, where relevant, cover the use of the student's name, photographs, voice (audio), image (video) and any other personal information disclosed in a film/ photograph.

3.16 The consent should make it clear who will be using the film/photograph (e.g., one or more of the School, AIS, CEC (or equivalent) and/or Diocese).

3.17 The consent should note that, if the student (or their parents) wishes to withdraw the consent, it is their responsibility to notify the School.

Other matters

3.18 Schools should carefully consider the purpose of sharing photographs and footage and limit recipients accordingly. For example, a class weekly journal should be limited to students, parents and teachers of that class, and not available to the whole School.

3.19 Extra care should be taken if a photograph or footage contains sensitive information. For example, if the individual's racial or ethnic origin or religious beliefs is apparent. Sensitive information must only be collected with the individual's consent.[3]

3.20 Schools should conduct appropriate due diligence on any platforms they will use to share photographs or footage, including ensuring the provider of the platform is subject to appropriate contractual obligations around access to, use of and protection of the photographs and footage.

3.21 If a parent or parents do not provide permission for a student in a particular cohort to be photographed or filmed in an activity which the school intends to make publicly available the school should give consideration whether to publicly release the photograph or footage if it would have the effect of precluding the student from participation in that activity.

3.22 It is recommended that each School develops a policy on use and sharing of student images, including the School's approach to obtaining consent.

[3]Consent can generally be implied where the student (or their parent as relevant) does not object to the photograph/footage being taken and understands why it is being taken, i.e., how it will be used and to whom it will be disclosed.

4. COUNSELLING RECORDS

General

4.1 From time to time issues arise in relation to the role of School Counsellors and their obligations to students. Other issues arise relating to the operation of the Privacy Act in relation to the record of personal information which is collected by Counsellors. This Section addresses these issues in the context of this Manual.

4.2 When reading these notes it is important to remember that:

(a) where a counsellor is employed by a school any records made by the counsellor in the course of their employment will be records of the school;

(b) counsellors do not have any 'legal privilege' in respect of their records which prevents these records being produced to a court if they are subpoenaed;

(c) while a school principal can require a counsellor to disclose information obtained in a counselling session to the principal or other senior staff, the disclosure should be limited to those staff members who have a need to know; and

(d) if the student discloses a sexual assault communications between the counsellor may be protected from disclosure to persons outside the School in criminal proceedings.

Under the *NSW Criminal Procedure Act 1986* (**Act**), **communications in confidence between Counsellors and victims of sexual assault,** referred to as 'protected confidences', are exempt from production under subpoena subject to certain exceptions.

(Note: Protected Confidences provisions do not change statutory reporting requirements in relation to either FACS or the Ombudsman.)

School Counsellors generally

4.3 School Counsellors may have different professional qualifications. Some will be registered psychologists, and members of the Australian Psychological Society or Australian Association of Psychologists, while others may have different professional qualifications such as in social work.

Professional Associations

4.4 It is not correct to say that the Codes of various professional bodies override obligations that a school Counsellor may have as an employee of a school or any contractual obligations to which the Counsellor may be subject. Neither do they override the provisions of the Privacy Act. Most Codes promulgated by professional associations appear to recognise this in varying degrees.

4.5 Often, necessary information can be conveyed to a person (i.e., School Principal) who has a legal obligation to receive it without betraying a confidence. However, there will be some occasions where it is necessary to directly pass on material to other staff which relates to the well-being of a student of the school.

4.6 In this context reference should also be made to Section 4 of Part D of this Manual which deals with 'Use or Disclosure of Personal Information'.

Effect of employment status of Counsellors

4.7 Employee

Where a Counsellor is employed by a School any records of personal information collected or made by the Counsellor will become records of the employer (the School). The School Principal is able to call for those records which directly pertain to a student of the school in the same way as he or she may call for the records made by any other School employee which relate to school matters. Those records may also be accessed by the student in accordance with the provisions of the Privacy Act unless they fall into an exception contained in the APPs. The question of access is discussed at Section 10 of Part D of this Manual.

4.8 Contractors

Where a contractor provides counselling services to the school, whether directly or through a third party agency, the question of who 'owns' any records will depend upon the relationship between the parties (ownership of records could be addressed in the contract with the contractor/third party agency).

However, as schools from time to time will require reports from the Counsellor about students it will be necessary for a 'collection notice' to encompass this collection, thus relieving the contractor of the obligation to provide a separate collection notice. It is suggested this notice should be provided to students and parents *before* a student uses the counselling service (e.g., when the School informs students and parents of the availability of the service, as well as when a student first uses the service). Schools could also consider including this in the general collection notice given by the school.

In addition to Privacy issues, from the standpoint of exercising its duty of care a School may also wish to include a provision in its agreement (contract) with the Counsellor to the following effect:

> *'The Principal may require you to provide him/her with the names of students to whom you are providing counselling services. In providing counselling services you must give detailed consideration as to whether the School may be able to give assistance to the student or students concerned or take action to prevent harm to the student. If the School may be able to give assistance or take action you must provide the Principal with sufficient particulars to enable the Principal to consider the relevant issues.'*

Under the Privacy Act, records of the contracted Counsellor may be able to be accessed by the student. Records held by the School which came from the Counsellor would be liable to be provided by the School to the student on request, subject of course to any exemptions contained in the APPs as mentioned earlier. (See Section 10 of Part D 'Access (APP 12)' and Section 5 of Part C 'Access to Records by Students and Parents').

4.9 Counsellors in Private Practice

Counsellors in private practice will generally be engaged by the parents of the child. In this case the relationship is between the child, the parents and the Counsellor. The School has no role to play except as requested by the Counsellor with the authority of the parents or student, or as requested by the parents.

Disclosure of reports

4.10 If the School makes a referral of a student, it may seek a report from the Counsellor. Where the Counsellor is a private practitioner the consent of the student (or in this case of a young student, the parent) may be required before that report could be provided.

4.11 Before a school counsellor enters into a counselling session with a student it is important that the student is provided with notice of:

(a) the nature of the services provided and that there is a choice to engage with the service, and

(b) the limits to confidentiality including that information shared in counselling may be disclosed to:

(i) the Principal and possibly other staff; and

(ii) subject to the comments below, parents.

4.12 If the student is thought not to be of an age or maturity that they would understand that they are consenting to this disclosure, should it be necessary, then the parents or guardian of the student should be given notice of the matters set out above. In determining whether this is necessary regard should be had to Section 7 of Part C 'Consent and Young People'. There may be times when this would be inappropriate, in which case the matter should be discussed with the Principal.

4.13 A draft form of Disclosure Statement to Students is attached at Annexure 8. Another, less formal approach, is for the counsellor to explain the process to the student and make a record that appropriate disclosures have been made to the student or parent. A template record form setting out the advice given is attached at Annexure 9.

4.14 If the student (or parent) chooses to proceed with the counselling session, they will be taken to have provided informed consent to the disclosure as outlined above.

Duty of Care

4.15 It is important for Counsellors to be aware that they need to work in conjunction with teachers at the School as a team so that both the Counsellor and the School can properly meet their obligations in relation to their duty of care. Where a Counsellor who is an employee, (and possibly a contractor depending on the terms and conditions of the particular contractual arrangement) fails to pass on relevant information and the student suffers injury as a result, the School may be found to be vicariously liable for the activity of that Counsellor. If a student fails to achieve the academic standards he or she may otherwise have achieved, had the School been aware of relevant material, the School may be found to be in breach of its contract to provide schooling with due care and skill.

4.16 Failure by a Counsellor to consult with relevant School staff, therefore, may have serious consequences for the School.

4.17 The issue of duty of care is referred to in Section 8 of Part C of this Manual – Duty of Care and Obligations of Confidence. In the context of duty of care, it is important to remember that the personal information is the personal information of the student, regardless of the age of the student. It can only be disclosed to parents if:

(a) disclosure is for the primary purpose of collection or for a directly related secondary purpose which is reasonably expected; or

(b) it is necessary to fulfil the School's duty of care to the student.

However, on occasions, even though disclosure to parents may be permitted, for example, as a reasonably expected directly related secondary purpose, the School Principal may decide not to do so because he/she has formed the view that disclosure may result in the child suffering harm.

5. ACCESS TO RECORDS BY STUDENTS AND PARENTS

This Section should be read in conjunction with Section 10 of Part D of this Manual - Access (APP 12).

Background

5.1 When a school receives requests from students and their parents to access personal information about the student, the school must respond to these requests. However, there are circumstances where access can be denied.

5.2 The requirement to provide an individual with access to their personal information is set out in APP 12 (and equivalents in the health records legislation if health information is sought). APP 12, including the exceptions to providing access, is considered in detail in Section 10 of Part D of this Manual - Access (APP 12). This Section provides further guidance on access requests.

Timing of response

5.3 A School must respond to a request for access to personal information within a reasonable period after the request is made. This is generally 30 days. The obligation is to acknowledge the access request, not to make the access decision, within a reasonable period.[4] Provided the School is actively dealing with the access request, and has acknowledged it within a reasonable period, the School has flexibility in how long it takes to provide (or refuse) access. However, Schools should act reasonably expeditiously.

When can parents access their child's personal information?

5.4 A parent can make a request to access their child's personal information under APP 12 if they are authorised to make the request on the child's behalf as a legal guardian or under authority from the child. The School will need to consider the student's age and capacity before responding to the request by a parent. If the information is not of a nature that is routinely provided to parents and the student has capacity to make the request, the School should generally seek the student's consent before providing the parent with access to the student's personal information. Section 7 of Part C of this Manual (Consent and Young People) provides guidance on age and capacity.

5.5 Where there are Family Court Orders in place, the schools needs to ensure that disclosure of the information is not inconsistent with these orders.

5.6 Where the parent requesting access is not authorised to make the request on the child's behalf, generally the School should not provide the parent with access, although there may be exceptions. In any event, the School must only provide access to the parent in this circumstance if the disclosure to the parent is permitted under APP 6 (see Section 4 of Part D of this Manual - Use or Disclosure of Personal Information).

5.7 The School's enrolment contract may also address when a parent is entitled to access the personal information of their child.

5.8 On occasions, the School may consider that providing a parent access to certain personal information may breach its duty of care by causing serious harm to the child. In this case, access can be refused.

When can a parent access the personal information of another child related to their child?

5.9 If a student is involved in an incident involving another student, a parent may ask to be informed how the School has responded to the incident, including what disciplinary action has been taken against the other student. The disciplinary action is the other student's personal information. The parent should only be provided with this information if this disclosure is permitted under APP 6 (see Section 4 of Part D –Use or Disclosure of Personal Information (APP 6)). Generally, it is recommended that parents are not informed of any disciplinary action taken against a student that is not their child, however, there may be exceptions in specific circumstances.

[4]'ZG' and Sydney Catholic Schools Ltd (Privacy) [2021] AICmr 89 and 'ZN' and a School (Privacy) [2021] AICmr 95 (17 December 2021).

Denying access on the basis of an unreasonable impact on the privacy of others

5.10 One of the main exceptions to providing access is where it would have an unreasonable impact on the privacy of others (APP 12.3(b)). This includes other students, parents, staff, consultants and other third parties.

5.11 Information could have an unreasonable impact on another person's privacy if it included any information about an individual which makes the individual "reasonably identifiable" (including when that information is combined with other information reasonably available to the individual who is requesting access). Personal information about an individual includes the individual's opinion or report of a matter, where the individual is reasonably identifiable.

5.12 Where a document contains the personal information of the requesting person as well as other people, it may be possible to provide it without identifying the other people by redacting some of the material.

Example

A student requested access to a report on an investigation, that contained the personal information of staff and students who provided evidence during the investigation. The School was able to create a redacted version of the report that removed the personal information of the staff and students and therefore was not able to rely on the exception in APP 12.3(b) to deny access to the report in its entirely. See further 'ZG' and Sydney Catholic Schools Ltd (Privacy) [2021] AICmr 89.

5.13 The following factors are relevant to whether the exception in APP 12.3(b) applies:

(a) the nature of the personal information about the other individual (e.g., whether it is of a sensitive or confidential nature);

(b) the reasonable expectation of the other individual about how that personal information will be handled, i.e. whether it would be disclosed to someone else (this may include what the School has told the individual, e.g., if a School informs a student who provides information in response to a bullying investigation, that the information will remain confidential);

(c) the source of the personal information (e.g., if the individual requesting access provided the personal information about the other individual);

(d) whether the personal information of another individual could be redacted from the record provided to the individual requesting access;

(e) whether access could be provided through an intermediary; and

(f) whether the other individual consents to access being given to the individual requesting access.

Example

A student made a request to a school to access their personal information relating to an incident that had occurred at the school. The school provided redacted documents. The OAIC found that the redactions were reasonable including because the subject matter was inherently sensitive, the parents that made the complaint would have a reasonable expectation that the personal information they provided to the school about their child and family would not be disclosed and, in relation to staff member's personal information, some of the communications were covered by an understanding of confidentiality among the staff. See further 'ZN' and a School (Privacy) [2021] AICmr 95 (17 December 2021).

Denying access on the basis of legal professional privilege

5.14 A School is not required to provide access to personal information where denying access is required or authorised by or under an Australian law (APP 12.3(g)). This includes where the information is subject to legal professional privilege (**LPP**).

5.15 A School may seek to rely on LPP where it has engaged a law firm to advise on a matter concerning a

student. However, Schools need to be careful to ensure LPP applies. In particular, Schools need to be careful when engaging law firms that they are engaging the law firm in its capacity as legal advisors, not in another capacity (e.g., as general consultants or investigators). It is recommended that this is documented (including the fact that any investigation is conducted for the purpose of the legal practice providing legal advice).

Example

A school undertook an investigation in relation to a complaint by a student. The school commissioned a report by an external investigator (a legal practice). The student sought access to this report from the school. The school refused to provide access on the basis of LPP (albeit the school did provide a summary of the report). The OAIC was not satisfied that LPP applied to the report as, amongst other things, the school advised the complainant that it was conducting an 'investigation' and had commissioned an 'investigator'; the author of the report conducted an interview with the student and introduced their role as having been engaged to conduct an investigation, and the legal practice described itself as *'a multidisciplinary legal practice'* and *'our team is made up of a diverse range of professionals, with expertise in supporting different aspects of organisational life. The are... lawyers, mediators, facilitators, investigators and HR specialists. We also have a team of expert consultants to call on so that we can respond appropriately to all your needs.'* The Commissioner was not satisfied that the report was a communication between legal adviser and client, nor that the report was produced for the dominant purpose of providing legal advice. The school did not provide evidence supporting its claim for LPP (e.g., correspondence between the school and the investigator). See further 'ZG' and Sydney Catholic Schools Ltd (Privacy) [2021] AICmr 89; cf 'ZN' and a School (Privacy) [2021] AICmr 95 (17 December 2021).

Denying access on the basis of existing or anticipated legal proceedings

5.16 Access can be denied where the information relates to existing or anticipated legal proceedings between the School and the individual, and the information would not be accessible by the process of discovery in those proceedings (APP 12.3(d)).

5.17 A legal proceeding is anticipated if there is a real prospect of proceedings being commenced, as distinct from a mere possibility. It is unlikely that a complaint will constitute anticipated legal proceedings.

Example

A school sought to rely on the exception in APP 12.3(d) on the basis that the individual had made a number of complaints regarding the school's decisions and procedure including to the school, the OAIC, the Australian Human Rights Commission, in a Federal Circuit Court application and to the Minister for Police and Emergency Services. The OAIC was not satisfied that APP 12.3(d) applied in such circumstances. See further 'ZG' and Sydney Catholic Schools Ltd (Privacy) [2021] AICmr 89.

Denying access on the basis that it would reveal commercially sensitive evaluative information

5.18 Access can be denied where giving access would reveal evaluative information generated within the School in connection with a commercially sensitive decision-making process (APP 12.3(j)). There are two limbs to be satisfied:

(a) the information must be evaluative in nature; and

(b) it must be generated within the School in connection with a commercially sensitive decision-making process. The decision-making process should involve commercially valuable information, the value of which would be diminished if the information were disclosed: 'ZN' and a School (Privacy) [2021] AICmr 95 (17 December 2021).

5.19 The exception applies only to the evaluative information, and not to personal information on which a decision was based.

Example

A student made a request to a school to access their personal information relating to an incident that had occurred at the school. The school provided access, but made redactions as the redacted parts of the documents set out *'the details of the [the School's] risk management strategy, plan, procedures, risk levels and evaluative information used by [the School] to manage the risks raised by the alleged incident in relation to all the children involved in the alleged incident'* and the relevant decision-making process (the determination of measures to be implemented to manage the risks raised by the alleged incident) was commercially sensitive due to the environment in which the school operated, including the potential for competition for enrolments. The OAIC accepted that APP 12.3(j) applied and permitted the redactions. See further 'ZN' and a School (Privacy) [2021] AICmr 95 (17 December 2021).

Access to health information

5.20 For Schools based in NSW, Victoria or the ACT, when a student or parent requests access to health information, the School should also consult the access requirements in the following legislation (as applicable):

(a) Health Records and Information Privacy Act 2002 (NSW);

(b) Health Records Act 2001 (Vic); or

(c) Health Records (Privacy and Access) Act 1997 (ACT).

6. DIGITAL LEARNING

Background

6.1 Schools increasingly use digital means to provide lessons and provide other aspects of schooling. For example, some Schools are:

(a) offering, or considering offering, remote lessons; and/or

(b) changing the way they collect, store and share student works and other materials associated with the classroom or a lesson. This includes the use of digital teaching environments (such as Google Classroom).

6.2 Care needs to be taken to ensure that privacy risks are considered when effecting these measures.

Remote lessons

6.3 Whilst remote lessons are not new, their use greatly increased during the COVID-19 pandemic, and some Schools may have reason to provide remote learning.

6.4 The privacy considerations differ depending on whether the remote lesson is recorded and, if it is recorded, what is recorded.

6.5 Where a remote lesson is not recorded, there are no additional requirements from a privacy perspective. The same considerations apply to the collection and disclosure of information as in a normal classroom. However, care should be taken to protect the students' (and household members') privacy generally. For example, asking students to use real names, blurred backgrounds, teacher monitoring attendance and screens on to identify attendees. The School should use a secure system for the remote lesson to avoid unauthorised attendees.

6.6 If a remote lesson is recorded, the School will be collecting and holding any personal information in the recording and must comply with the Privacy Act (and health records laws if health information is recorded) in relation to the recording. Other laws may also apply, such as surveillance devices legislation and the *Copyright Act 1968* (Cth).

6.7 Schools should only record a lesson if the recording is reasonably necessary for the School's functions or activities. That is, recordings generally should not be made just because they may be useful for an unknown purpose in the future.

6.8 If Schools do record a lesson, it is recommended that the lesson is pre-recorded by the teacher only (i.e., without students). If a live lesson needs to be recorded, the School should ensure that only the teacher can be seen or heard. If a School wishes to record a lesson in which a student (or other person) can be seen or heard, it is recommend the School seek advice on any steps it needs to take to permit this and to ensure the secure transfer of the recording to the intended recipient.

6.9 Schools should also consider whether their approach to remote lessons should be reflected in their privacy policy and privacy collection notices – see Section 1 of Part C – Privacy policies and collection notices.

Digital collection, storage or sharing of materials associated with a classroom or lesson

6.10 Schools are using a variety of digital platforms to collect, store and share materials associated with a classroom and/or lesson (e.g., digital teaching environments like Google Classroom). This could include things such as class lists, student works and documents that teachers may need to refer to in class (e.g., a teacher development plan, student allergy plan and student learning plan).

6.11 Given the variety of platforms used, and the different ways Schools use these platforms, it is not possible to set out detailed recommendations in this Manual. However, the following principles can be used to guide Schools on their own assessment of their use of the platforms:

(a) **transparency**: be transparent with students and parents about the platforms used. Where a new platform is introduced, consider notifying students and parents of this, including what personal information will be handled through the platform and why, who can access the personal

information and where it will be stored. Also consider whether the School's privacy policy and privacy collection notices need to be updated to address the platform. See further Section 1 of Part C – Privacy policies and collection notices;

(b) **limit uploading**: carefully consider whether there should be limits on what staff can upload to the digital platform, in particular whether sensitive information (or information of a sensitive or confidential nature) should be uploaded. For example, the School may decide that documents such as teacher development plans and student behaviour plans should remain on the School's secure systems that are only accessible by School staff;

(c) **limit sharing**: carefully consider what should be shared from the platform and to whom (this includes who can access information in different parts of the platform). For example, student works should only be shared with students in the relevant class, not all students at a School. Consider whether particular documents should be shared by other, more secure, means;

(d) **teach students**: explain to students (and potentially parents) who can access personal information that they share through a platform and how they can limit access if they wish (e.g., the choice between sharing with teacher and sharing with the whole class). Also teach students how to protect their access to the platform (e.g., how to choose a password and keep it secure);

(e) **train staff**: train staff on the appropriate use of the platform (including to address the matters in points (b) and (c) above and security, e.g., not leaving their computer unlocked in the classroom, how to choose a password and keep it secure);

(f) **security**: ensure the personal information is secure on the platform (i.e., it is protected from misuse, interference and loss; and from unauthorised access, modification or disclosure). This includes, for example:

(i) assessing the security of the platform and the security reputation of the platform provider;

(ii) imposing appropriate contractual obligations on the platform provider (where possible); and

(iii) ensuring access controls are in place (including limiting access on a need to know basis, and ensuring the access mechanism is secure, such as multi-factor authentication). This includes access by staff, students and parents. See also Paragraphs (d) and (e) above.

See further Section 9 of Part D – Data security;

(g) **storage location**: ensure the School is aware where information in the platform is stored/hosted and, where there is an overseas disclosure, the School complies with APP 8. See further Section 6 of Part D – Cross-border disclosure of personal information;

(h) **quality/correction**: ensure mechanisms are in place to ensure the personal information is accurate, up-to-date and complete. This is particularly relevant if the personal information is stored both in the School's systems and in another platform, as the School will need to make sure the information is correct in both locations;

(i) **delete**: delete or de-identify any personal information on the platform when it is no-longer needed for a permitted purpose. See further Section 9 of Part D – Data security;

(j) **access requests**: make staff aware that anything they type into the platform is potentially collected and held by the School, and may be subject to an access request by a student (or their parent). This is particularly important if the platform has a chat function;

(k) **data breach response**: consider how the School will respond to a data breach involving the platform and how the School will obtain the platform provider's assistance in responding to the breach. This also includes managing data breach notification with the provider. It is recommended this is addressed in the contract with the provider. See further Part B – Data breaches; and

(l) **policy**: consider whether the School should develop a policy in

relation to the use of the platform, to formalise the matters above.

6.12 This list is provided as guidance only. It is not an exhaustive list of the matters that should be considered as this will depend on the circumstances. It is recommended that a privacy impact assessment is conducted for any new platforms through which personal information will be collected, stored or shared. Depending on the circumstances, this may be required by APP 1.

6.13 Whilst this section is focused on platforms used for digital learning, many of the factors above are also relevant to any new digital platform a School plans to use (e.g., a new platform to collect and process enrolment applications).

School approved email and platforms

6.14 Schools should ensure that policies and procedures (including staff training) are in place to ensure that staff only use School approved email and platforms to store and share personal information.

7. CONSENT AND YOUNG PEOPLE

7.1 The Privacy Act does not distinguish between adults and children and thus clearly envisages that young people are to be afforded rights in respect of their privacy. However, the APPs do not differentiate between children of different ages and thus it is difficult to determine when it is appropriate to seek consent from students.

7.2 In relation to consent and young people, the OAIC's guidance 'Children and young people' provide as follows:

> *The Privacy Act 1988 protects an individual's personal information regardless of their age. It doesn't specify an age after which an individual can make their own privacy decision. For their consent to be valid, an individual must have capacity to consent.*

An organisation or agency handling the personal information of an individual under the age of 18 must decide if the individual has the capacity to consent on a case-by-case basis. As a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what's being proposed. If they lack maturity it may be appropriate for a parent or guardian to consent on their behalf.

If it is not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, as a general rule, an organisation or agency may assume an individual over the age of 15 has capacity, unless they're unsure.

7.3 The Australian Law Reform Commission (**ALRC**) also considered the issue of consents by children and young people and recommended that the Privacy Act should be amended to provide that where an assessment of capacity to provide consent 'is not reasonable or practicable' an individual of the age of 15 or over should be capable of giving consent and a person under that age should be presumed not to be capable of giving consent.

7.4 The ALRC also noted that people with parental responsibility had some authority to make decisions on behalf of their children who lacked capacity if it was part of a duty to provide for their welfare but did not suggest that such authority extended to all situations.

7.5 In approaching the issue of privacy for Schools it is important to remember that the underlying arrangement between the School and parents is contractual. Parents are engaging the School to provide schooling for their child on the terms agreed by the parties. The School's authority over the child derives from the contract with the parents and its legal obligations.

7.6 A parent is recognised by the common law as having the right to make decisions concerning the child's education and to bring up their child in the religion of their choice. In all States and Territories the age of majority is 18 years.

7.7 For these reasons, one approach would be for the School to adopt the view that in many circumstances, the contract with the parents will govern their relationship with the child in relation to privacy, and thus consents given by parents will act as consents given on behalf of the child and notice to parents will act as a notice given to the child.

7.8 However, this approach will not be appropriate in all circumstances. A School should recognise that young people do have rights under the Privacy Act and in some circumstances it would be appropriate to seek consents from them, particularly when they are aged 15 or over, as indicated by the APP Guidelines and ALRC. No doubt in most cases decisions whether to seek information or consents from students or from parents is likely to follow current practices. Thus, for example, where a student puts his or her name down to take part in a team, the student would usually be impliedly consenting to it being disclosed to a relevant party to enable him or her to compete. As a student reaches greater maturity, the more important it will become to consider whether a parent should be asked for consent or the student. Hopefully in most cases common sense will provide the answer.

7.9 For example, in most cases it would be appropriate for the School to collect from a mature student personal (and sensitive) information about the student gained through an interview with the student. Also, there will be many instances throughout a student's schooling where it would be impracticable and inappropriate to first obtain a parent's consent when collecting personal information from a student (e.g., during day to day classroom activities). In respect of collecting personal information about students from parents, it is suggested that it is sufficient if parents are given a collection notice informing them of the requirements set out in APP 5.2 and students do not need to be specifically and separately informed.

7.10 Another potential concern is that students seek to prevent disclosure of personal information to a parent, such as their School report. The Standard Collection Notice in Annexure 6 of this Manual seeks to overcome this by informing students and parents that the School will disclose personal information about a student to the student's parents. If a student attempted to restrict disclosure of personal information (such as a School report) to a parent, it is reasonably clear that providing a report would be a permitted purpose as being a related purpose to the purpose for which the information was collected. However, this does not prevent the School exercising its discretion to restrict disclosure of the personal information. There are occasions when Schools do agree to not provide a student's personal information to a parent at the request of the student, such as when the parents are separated and the student has a bad relationship with the non-custodial parent.

7.11 See Sections 5 of Part C and 10 of Part D of this Manual in relation to students and parents seeking access to their or their child's personal information which is contained in records held by the School.

7.12 Particular issues may arise in the context of information provided to staff members, including counsellors, by students 'in confidence' that is, where the student has asked or expected the staff member not to disclose it. This is discussed more fully at Section 4 of Part C. However, one factor when considering how to deal with such situations will be the age and capacity of the students to provide or refuse consent.

8. DUTY OF CARE AND OBLIGATIONS OF CONFIDENCE

Duty of Care, Obligations of Confidence and the APPs

8.1 As will be discussed in Section 3.57 of Part D of this Manual, a School generally can only collect sensitive information (including health information) with consent and can only use and disclose personal information for the purpose for which it was collected or a directly related secondary purpose. There are two important relevant exceptions to those general rules:

(a) where the person consents; and

(b) where required or authorised under a law.

8.2 The Privacy Act specifically provides that in this context, 'law' includes the common law. The common law imposes a duty of care on Schools which they must exercise in relation to students and staff. It can be contended that Schools are required by this common law (duty of care), to collect certain personal and sensitive information in order to comply with this duty. This would justify the School collecting sensitive information about students and possibly others (e.g., parents, contractors etc.) under APP 3.2 in order to fulfil its duty of care in its responsibility as the carer and educator of children. A duty of care may also permit use and disclosure under APP 6 in circumstances where such disclosure would not be reasonably expected.

Example:

An example of where a duty of care may require disclosure would be where a School informs a third party temporarily responsible for a student that the student suffers from a particular health problem.

8.3 The common law, in some situations, imposes upon people an obligation of confidence. In broad terms, confidence can be claimed where:

(a) the information is by its nature confidential;

(b) the information is communicated in circumstances importing an obligation of confidence; and

(c) disclosure of the information would be unauthorised by the provider or by law.

8.4 If personal information is given in confidence it is clear that the provider would not wish it to be used by the School or disclosed by the School for purposes other than the purpose for which it was given. However there may be occasions where such confidence can be breached if this is required in order for the School to fulfil its duty of care.

8.5 Personal information provided by another person in confidence may still need to be disclosed if the subject of that information requested it from the School under APP 12, as such disclosure may be authorised under law.

8.6 The uncertainty in this area only serves to underline the fact that records of confidential information should only be made where there is a need to do so and in the knowledge that access to the record may be sought.

8.7 A common law duty of care and obligation of confidence might be used to restrict an individual's access to records of personal information held about them in some cases.

Example:

An example of when confidential information may be withheld may be where a student has advised a teacher of a particular home situation where disclosure to the parent the subject of the information may cause adverse repercussions for the student. This is not because it was confidential so much as because of the School's duty of care to the student. It may also have an unreasonable impact on the privacy of the student (APP 12.3(b)).

9. DISCLOSING AND USING PERSONAL INFORMATION WITHIN THE SCHOOL COMMUNITY

Passing information in a School Community

9.1 Schools create 'communities'. The School community will typically consist of staff, students, parents, past students and benefactors. Where the School is affiliated with a particular religion, a minister, the church and the congregation will often be included in the broader school community.

9.2 As in any community, information about others is passed through the community and on occasions will be recorded. Thus a note from a School Principal to a priest that a child or child's parent who is a regular member of the church congregation is sick may not be unusual. Technically this could not be done without the consent of the parent (and/or child as relevant). However, if the Principal is confident consent would be given, or indeed the passing on the information would be expected, then failure to adhere to the 'letter of the law' would be unlikely to have any repercussions.

9.3 In the same vein, a note in a newsletter asking the community to pray for a sick child or sick parent may involve a 'technical breach' of the APPs if it involved disclosure of sensitive information but is unlikely to cause offence. However, on occasions it may cause offence, particularly if the individual wished their illness to be kept confidential, therefore caution should be exercised in this regard. If the School is unsure if the individual (or their parent as relevant) wishes for the illness to be kept confidential, the School should check with the individual (and/or their parent as relevant).

9.4 It should also be borne in mind that where such practices are well known in the community, consent to collection may well be implied in many circumstances and disclosure may be reasonably expected (albeit the disclosure would also need to be related, or directly related for sensitive information, to the purpose for which the information was collected).

9.5 The guiding principle in such cases is to show sensitivity in exercising a judgement as to when it is appropriate to disclose this type of information.

Religious Information

9.6 Where religious information about an existing or potential student or parent is sought from a priest or minister, it would be wise to obtain consent. In most cases, this can be achieved in appropriate applications or enrolment forms. However, where practicable and reasonable, the School would collect religious information directly from the student or parent.

Fundraising

9.7 Disclosure of information for fundraising purposes raises greater difficulty. However, it is suggested that non-government schools usually rely on extra funds raised via approaches to parents and Alumni and that this would be a reasonably expected related secondary purpose. However, to ensure that it is expected it would be wise to include that fact in a collection notice. This activity is referred to in the sample 'standard collection notice' in Annexure 6.

School directories

9.8 The use and disclosure of school directories and class lists which contain students' and parents' name and contact numbers and similar information (e.g., enrolled class) may involve the disclosure of personal information to others. Such a use of individuals' personal information may not be reasonably expected by the individual concerned. To avoid any doubt Schools should obtain the consent of parents (on their own and their child's behalf) to place their details in the School Directory or class list. Alternatively, the School could notify parents (and children) about such practices in a 'standard collection notice' (see Annexure 6 of this Manual). Experience has shown that some parents do not want their details to be included on class lists, and therefore it is recommended that Schools obtain consent rather than relying on the notice provided in a standard collection notice.

School publications and other news

9.9 School publications, such as newsletters, magazines and alumni publications usually contain personal

information obtained either from the relevant individual or from other sources.

9.10 Provided the Standard Collection Notice in Annexure 6 of this Manual is provided to students (or their parents as relevant), Schools can share personal information (other than sensitive information[5]) with current, future and past students, parents and teachers for the purpose of reporting on school activities and events. The minimum amount of personal information should be shared as part of the report.

9.11 To share news and events that includes personal information with a broader audience, or to specifically promote the School, the School should generally seek consent. It is recommended that Schools utilize:

(a) an annual general consent form (with separate tick boxes) that is completed at the beginning of each school year. An example is in Annexure 7; and

(b) a specific consent form for particular situations which may not be covered by the general consent.

9.12 For further information on the sharing of videos and footage, please refer to Section 3 of Part C of this Manual.

9.13 Health information should not be included in school publications without consent.

Library collections

9.14 The Privacy Act excludes '*anything kept in a library … for the purposes of reference, study or exhibition*' from the definition of 'record'. Thus the APPs do not apply to material contained in library collections.

Systems and Schools conducted by Church Bodies

9.15 The non-government school sector includes a large number of systems. These are predominantly Catholic education systems, although a number of other religious denominations conduct schools as part of a 'system'.

9.16 The system model may involve the conduct of a number of schools by the one legal entity (which is generally the Catholic model) or the conduct of a number of schools which have separate legal entities but 'report' to a central authority and are ultimately subject to its direction. In both cases many functions are centralised.

9.17 A Diocese is not a 'related body corporate' of another Diocese, as this term is confined to the definition contained in the Corporations Act. Each Diocese is incorporated by an Act of Parliament and is created as a separate legal entity.

9.18 Where a system consists of separate legal entities then these will be separate organisations. In some cases they also may be related bodies corporate.

9.19 Personal information can be used and disclosed within a system where there is one legal entity, or within a system which consists of related bodies corporate, for the purpose for which it is collected (in respect of related bodies corporate, it is the purpose for which the first organisation collects the information).

9.20 Roman Catholic Orders that conduct Schools are generally incorporated under State Acts and their affairs are managed by Trustees. In these circumstances they are not 'related bodies corporate' to other Catholic Orders within the meaning of the Corporations Act. Nor are they related to the various Catholic Dioceses.

9.21 When a School is not related to a second School it cannot rely upon section 13B of the Privacy Act (the related bodies corporate exemption) to disclose information to that second School. However, it can still use the provisions relating to consent or related and reasonably expected secondary purpose. In most cases the practical outcome will not be different.

[5]Extra care needs to be taken with sensitive information (including religious beliefs) to ensure that the purpose for which the information is shared is directly related to the purpose for which it was collected, and reasonably expected by the individual. It is recommended this is assessed on a case by case basis.

10. SHARING INFORMATION WITH OTHER SCHOOLS

10.1 Where another School which is not within the same system (i.e., not part of the same legal entity) or is not a related corporation requests personal information about a student at a School, in usual circumstances this information should not be passed on without consent. It may be done on occasions as part of the School's duty of care. Schools which are related entities may share personal information other than sensitive information, subject to restrictions on its use, although it is advisable to obtain consent in any case where practicable to do so.

10.2 The Interstate Student Data Transfer Note (**ISDTN**) and Protocol was established under the *Schools Assistance (Learning Together Through Choice and Opportunity) Act 2004*. The purpose of the initiative, between the Australian Government, State and Territory Education Departments, and the Independent and Catholic education sectors, is to allow for the transfer of student information between schools when children move from one state to another and to provide 'flags' for the new school regarding educationally significant information about the student.

10.3 Under the ISDTN and Protocol, when a new student from another state enrols or applies for enrolment, the new school will follow a process to request the transfer of information from the student's previous school. The key aspect of this system is the circumstances in which the parent or student is required to give consent.

10.4 The ISDTN and Protocol set out the processes by which schools must obtain consent from the parent/guardian and in some cases, the student, before information can be collected from the student's previous school.

10.5 The consent regime is as follows:

(a) where the information is to be passed from one non-government school to another, parent or student consent is **not required** before the information can be passed if the previous school has a data collection notice which conforms to the Standard Collection Notice in Annexure 6 of this Manual;

(b) where the information is to be passed from a government school to a non- government school, the new school must collect consent before requesting the information from the previous school; and

(c) where the information is to be passed from a non-government school to a government school, the obligation falls on the new school to collect the consent before it can request the information from the previous school. The non-government school should require the government school to demonstrate that is has obtained consent before disclosing any personal information to the government school.

10.6 Information about the ISDTN and Protocol and the relevant consent forms can be found at the Department of Education's website at

https://www.education.gov.au/transferring-student-data-interstate

11. DISCLOSURE OF INFORMATION WHERE REQUIRED BY LEGISLATION

11.1 In New South Wales, the following legislation may permit or require the disclosure of personal information about students, staff, parents or others.

(a) Chapter 16A of Children and Young Persons (Care and Protection) Act 1998;

(b) Children's Guardian Act 2019;

(c) Part 5A of the *Education Act 1990* (Health and Safety risks of schools arising from student behaviour); and

(d) Child Protection (Working with Children) Act 2012.

11.2 In other States and Territories, the following legislation may permit or require the disclosure of personal information about students, staff, parents or others:

(a) ACT: Children and Young People Act 2008 and Education Act 2004;

(b) Queensland: Child Protection Act 1999, Working with Children (Risk Management and Screening) Act 2000, Education (General Provisions) Act 2006, Education (Queensland College of Teachers) Act 2005; and Western Australia: Working with Children (Criminal Record Checking) Act 2004, Teacher Registration Act 2012, School Education Act 1999, Children and Community Services Act 2004, Parliamentary Commissioner Act 1971, Commissioner for Children and Young People Act 2006.

11.3 There may be similar legislation in other States. You are advised to check what legislation applies in your State.

12. CONTRACTORS

12.1 Schools sometimes enter into contractual relationships with another party (the contractor) in which the contractor:

(a) supplies services to the School; or

(b) supplies services to someone else on behalf of the School;
and the contract involves the contractor handling personal information.

12.2 The Privacy Act treats the acts and practices of employees (and those 'in the service of' a School) in performing their duties of employment as those of the School. Contractors performing services for a School are not considered to fall within this provision. However, where there is a particularly close relationship between the School and a contractor it may mean that the actions of the contractor could be treated as having been done by the School. In certain circumstances, a School may also 'hold' personal information that a contractor has possession of, as the School has control over the information, and the School will have obligations under the Privacy Act in relation to that information.

12.3 In practical terms there may be little difference in what the School needs to do to meet its obligations.

Disclosure to contractors

12.4 In circumstances where the School and a contractor are separate entities under the Privacy Act, and where the School gives personal information to a contractor, the School has 'disclosed' that information, and the contractor has 'collected' the information. In practical terms, this means that the School should have clauses in the contract for the protection of personal information it discloses to the contractor, in order to meet its obligations under the APPs. Depending on the nature of the personal information provided to the contractor, the School may also need to conduct due diligence on the contractor and audit the contractor's compliance with the contractual obligations that the School imposes.

12.5 In limited circumstances, providing personal information to a contractor may be a use, rather than a disclosure. This occurs when the School does not release the subsequent handling of the personal information from its effective control. However, the steps a School needs to take to protect personal information are similar regardless of whether the provision of the personal information to the contractor is a 'use' or a 'disclosure.'

12.6 Schools should ensure that contractors are only provided with, or provided access to, personal information that they need for providing the relevant service to the School.

Making the individual aware of the contracting arrangement

12.7 When the School contracts out functions or activities, both the School and the contractor have obligations under APP 1.4 and APP 5.2 to make an individual aware of certain information.

The Contracting Organisation (School)

12.8 Where the School usually discloses personal information to a contractor, the school must take reasonable steps to ensure that the individuals from whom it has collected information are made aware of these disclosures (APP 5.2(f)). The steps the School takes to inform individuals that personal information about them will be disclosed to contractors will depend on the circumstances. It may be enough to include in the 'standard collection notice' (see Annexure 6) a statement that 'The School occasionally uses contractors to assist the School in its functions and discloses relevant personal information to these contractors to enable them to meet their obligations'. Whether this is sufficient will depend on the nature of the services provided by the contractor and the type of personal information they handle.

12.9 What other details about the contractor and relevant to APP 5.2 of which the School makes an individual aware will also depend upon the circumstances including what the School and the contractor have agreed between them. However, such arrangement must not detract from the individual's privacy rights.

The contractor

12.10 There are a number of ways in which a contractor collecting personal information under a contractual arrangement could meet its obligations under APP 5.1 (to take such steps (if any) as are reasonable in the circumstances to notify the individual of APP 5.2 matters). The contractor does not necessarily need to notify individuals itself. The School that originally collects the personal information could notify individuals that information about them will be disclosed to the contractor, and other relevant details including the purpose for which the contractor will use the information, and how individuals can contact the contractor.

12.11 In some cases, it could be reasonable for no steps to be taken under APP 5.1 (other than referring to the fact that the School uses service providers to handle personal information on the School's behalf in the standard collection notice).

Collecting sensitive information under a contract

12.12 A contractor that collects sensitive information would generally need to have the individual's consent. Often the contractor will require the School to obtain such consent on the contractor's behalf.

APP 6: Use and disclosure of personal information

12.13 Where the School proposes to disclose personal information under a contract, it would need to consider how APP 6 applies to the disclosure. In some situations where the School contracts out a function or activity, the disclosure will be for a primary purpose of collection or an activity that is related to the primary purpose and within the individual's reasonable expectations (e.g., mailing activities).

12.14 Where the School discloses personal information to a contractor to carry out activities that fall outside these categories then, in most cases, the School would generally need the individual's consent under APP 6.1(a).

12.15 One way of reducing this risk is to ensure that the contract includes very clear provisions about the purpose for which the contractor is to use the information and other provisions necessary to ensure the contractor does not make unauthorised uses or disclosures. It should also have provisions about how the contractor is to keep the information secure, and what it must do with the information when it has completed the contracted out activity.

APP 11: Security of personal information

12.16 APP 11 requires a School to take reasonable steps to protect the personal information held from misuse, interference and loss, and from unauthorised access, modification, or disclosure. It would be advisable where the School contracts out a function or activity to include in the contract provisions to assist in complying with APP 11 (and requiring any subcontractors to agree to similar provisions).

12.17 A contractor which collects personal information from the School would usually have obligations of its own under APP 11 to keep the information secure.

Notifying Data Breaches

12.18 The contract should require the contractor to notify the School if there is a Data Breach that affects personal information it holds and provide all reasonable assistance to the School in responding to any Data Breach (including in relation to gathering the information required for notification to the OAIC and individuals if there is an eligible data breach (**EDB**) and amending its practice to ensure that data breaches do not occur in the future).

12.19 The contract should also make clear who is to notify the OAIC and individuals if there is an EDB under the notifiable data breaches scheme (see Paragraph 1.15 of Part B).

13. SCHOOLS AS CREDIT PROVIDERS

13.1 Schools may be recognised as 'credit providers' under the Privacy Act.[6] A School will be treated as a credit provider for the purposes of the privacy legislation only where it provides credit in connection with the supply of goods or services and agrees to defer repayment of the credit, in full or in part, for at least 7 days. Providing credit means agreeing to defer payment of a debt owed or incurred.

13.2 By way of example, a School is likely to be considered to be a credit provider where it:

(a) expressly permits a parent to defer payment of school fees for a period of at least 7 days beyond the due date (the date stated for payment on the invoice); or

(b) allows school term fees to be paid at least 7 days after the school term commences.

13.3 In practice, whether a School has provided credit by deferring payment of school fees will be a question of fact and an assessment would need to be made on a case by case basis.

13.4 The OAIC has indicated that for the purpose of interpreting the 7 day term, the following guide is appropriate:

(a) Day 1 is the day on which the goods or services are provided.

(b) Day 8 is the day on which payment is due.

This is consistent with the view that a debt is deferred if a contract allows the debtor to pay later than the time the benefit is supplied to the debtor under the contract, i.e., a School permits school term fees to be paid at least 7 days after the school term commences.

13.5 However, whether a School is a credit provider may ultimately depend on the terms of the contract or arrangement between the School and the student's parents in relation to school fees. For example:

(a) A School may not be considered to be a credit provider where it expressly permits the payment of school fees in three equal instalments across the school term. Prior to the third payment, the student would not have received the benefit bargained for and consequently there is no deferment of debt, as each debt arises at the time the instalment is due, and payment is made at the time.

(b) Conversely, a School may be a credit provider if school fees are due 7 days after the school term commences, but the school permits payment in equal instalments. The School has permitted payment at a time later than the time at which payment would ordinarily be due under the contract, and as such, payments permitted after the due date would constitute a "deferred debt".

13.6 If it is recognised as a credit provider, the School will be treated as one only in relation to that particular provision of credit. This will mean the School will be required to comply with additional obligations under the Privacy Act and the Credit Reporting Code in relation to that particular provision of credit. Criminal offences and civil penalties may also apply if a School breaches these obligations.

13.7 One of the key obligations is for credit providers to have a policy about the management of "credit information" and "credit eligibility information", which sets out (amongst other things) the purposes for which the credit provider collects, holds, uses and discloses these types of information. A School must ensure this policy is easily accessible (for example, available on the School's website). These are similar to the privacy policy obligations a School has under APP 1 as explained further in Section 1 of Part D of the Manual.

[6]This Section 13 only relates to whether a School may be a credit provider under the Privacy Act. It does not address Schools that might be credit providers regulated by the National Credit Code (which is Schedule 1 of the *National Consumer Credit Protection Act* 2009 (Cth)). If a School is unsure if it is a credit provider regulated by the National Credit Code, or of the implications of this, the School should seek legal advice.

13.8 The extent of a School's obligations will be determined by the extent to which it participates in the credit reporting system. That is, whether the School discloses information to, or receives information from, credit reporting bodies (e.g., request a credit report about a parent), other credit providers or other third parties, including debt collectors, or wishes to list defaults with a credit reporting body. As noted above, this information must be set out in the School's credit reporting policy.

13.9 It is believed that most Schools are unlikely to be substantial participants in the credit reporting system and accordingly, their obligations will be minimal. If they do none of the things set out in Paragraph 13.2 of this Part C they only need to state in their privacy policy "*The School does not collect personal information from credit providers or credit reporting bodies*".

13.10 Schools should obtain legal advice (or contract AIS or CSNSW) if they have concerns about these provisions.

14. EMPLOYEE RECORDS

14.1 An act done, or practice engaged in, by a School that is or was an employer of an individual is exempt from the scope of the Privacy Act if the act or practice is directly related to:

(a) a current or former employment relationship between the School and the individual; and

(b) an employee record held by the School relating to the individual.

14.2 An 'employee record' is defined broadly to be a record of personal information relating to the employment of an employee. Examples of employee records include information about:

(a) the health of the employee;

(b) the engagement, training, disciplining or resignation of the employee;

(c) the termination of the employment of the employee;

(d) the terms and conditions of employment of the employee;

(e) the employee's personal and emergency contact details;

(f) the employee's performance or conduct;

(g) the employee's hours of employment;

(h) the employee's salary or wages;

(i) the employee's membership of a professional or trade association;

(j) the employee's trade union membership;

(k) the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and

(l) the employee's taxation, banking or superannuation affairs.

14.3 There is a similar exemption in New South Wales for health records of an employee. In particular, health records will not be considered to be 'personal information' under the *Health Records And Information Privacy Act* 2002 (NSW) and will not be covered by that legislation. In the Australian Capital Territory and Victoria, there is no such exemption in relation to the collection, use and disclosure of an employee's health records. If the ACT or Victorian legislation applies to your School, see Paragraphs 2.20 - 2.25 of Part C of this Manual.

Circumstances where the exception does not apply

14.4 The employee records exemption does not extend to prospective employees, contractors, consultants or volunteers.

14.5 In addition, the exemption does not apply until the personal information is held by the School. As such, Schools must comply with the Privacy Act when collecting personal information (including obtaining consent to collect sensitive information). Requirements that apply to the collection of personal information are explained in Section 3 of Part D of this Manual.

14.6 The exemption will only apply to an employee record held by the employing organisation. Once the record is disclosed to another entity, the exemption will cease to apply and the APPs will govern the handling of that information in the hands of the new entity holding the record. This is of particular importance where a School has access to employee records (for example via a database, or centralised HR facility) of employees of a School operating a related body corporate. In such cases, the School which is not the employer of the individual to whom the records relate will be subject to the requirements of the Privacy Act in using and disclosing those employee records. It also means that where one School in a group of separately incorporated related Schools retains employment information for the group, the employees of the other Schools *will* be able to access (under APP 12) their personal information because the School holding their personal information is not their employer.

14.7 Acts of employers who use employee information for commercial purposes outside the employment context will not be exempt from the operation of the Privacy Act.

14.8 Whether or not information of this nature will be considered as being 'directly related' to the employment relationship will be a question of fact to be decided in the context of each case. However, the School should

bear in mind the consequences of having information which falls outside the employee records exemption (i.e., the Privacy Act applies to the School's handling and protection of the information, and the School must provide the employee with access to the information on request, unless an exception applies).

14.9 Where a record of employee personal information falls outside the employee records exemption and is subject to the Privacy Act, then it is only that part of the record which falls outside the exemption that will be subject to the Privacy Act and not the whole record.

14.10 As the employee records exemption does not apply to job applicants, job applicants may seek access to and correction of records of their personal information which the School holds about them. The School should be mindful of this when collecting personal information (e.g., references, making notes and reports).

Disclosing employee information to an AIS or Catholic Offices (and employee access to such information)

14.11 It is common for names of employees to be given to organisations such as the AIS in order to, for example, enable the AIS to provide advice to the School in relation that employee. (Catholic Offices on occasion also give advice to non-systemic Schools. These offices do not, however, have the benefit of legal professional privilege). If you are unsure about the application of legal professional privilege, you should seek legal advice first.

14.12 In this scenario, issues may arise as to:

(a) whether the AIS is required to give a collection notice to the employee;

(b) whether the employee can access the record; and

(c) what the AIS should do with the record after the advice is given.

14.13 In most cases, it would be reasonable *not* to provide a collection notice as the disclosure relates to an employee record, it is provided confidentially, and it is used for a very limited purpose and providing a notice may frustrate the purpose of obtaining advice.

14.14 If an employee of a School sought access to the material from the AIS or Catholic Office, there are a number of grounds on which access could be denied (see Section 10 of Part D of this Manual). After the issue is finalised, the AIS or Catholic Office should de-identify the information or destroy it if there is no reason to retain the information. If the AIS or Catholic Office is unsure if there is a legal reason to retain the information, they should seek legal advice.

Recommendation

14.15 In situations where the employee records exemption does not apply, Schools should consider what steps they need to take to comply with the Privacy Act. The other sections in this Manual should guide the School on these steps.

14.16 Regardless of whether the exemption applies, Schools should protect employee records and take steps to ensure they are only used for employment related purposes (unless another purpose is permitted under the Privacy Act).

14.17 If employee records are disclosed to a third party, the School should be aware that it will not be an 'employee record' in the hands of that third party and a collection notice may need to be given by or on behalf of the third party. In addition, the employee will be able to access the employee record from the third party (unless another exemption applies).

14.18 Where employee records are given to third parties to enable them to provide advice, an issue of access may arise. Consideration would need to be given to whether there are grounds for resisting access.

14.19 Information provided to a central Catholic Education Office about employees in different schools remains in the hands of the one employer. If it is disclosed to another Catholic Education Office, an issue may arise as to whether a collection notice should be given by that second office. This situation is clearly distinct from information handling in the AIS environment.

15. TRANSFERS BETWEEN RELATED COMPANIES

15.1 A related company or 'related body corporate' is defined under the Corporations Act as either a holding company or subsidiary of another body corporate, or a subsidiary of a holding company of another body corporate.

15.2 Essentially, a related company refers to businesses that have a shared controlling interest. There will not be many Schools that will be related bodies corporate to other Schools within the definition in the Corporations Act. Where a number of schools are operated by a single legal entity (a system of schools) the information will be held by the legal entity. If the schools are separately incorporated but have a common membership, they will be regarded as related bodies corporate. Particular issues arise in this regard for school systems which may be based on religious structures such as Dioceses and separately incorporated Orders. It is unlikely that separately incorporated Orders would be recognised under the Corporations Act as a related body corporate of a Diocese.

15.3 In many circumstances, Foundations and Trusts which are separately incorporated and established by a School are likely to be related bodies corporate of the School.

15.4 Under the Privacy Act, a company that is related to another company will be able to share personal information (**but not sensitive information**). However, those related companies must still comply with the APPs in relation to the shared personal information.

15.5 The primary purpose of collection of the personal information of one body corporate will be deemed to be the same as that of the related body corporate which receives the information.

15.6 Therefore, that information may not be used for any other purpose, other than the same primary purpose for which the information was collected by the original body corporate (or a related secondary purpose that the individual would reasonably expect).

15.7 As the related bodies corporate exemption does not apply to the sharing of sensitive information, and given that a large part of information that Schools collect and use is sensitive information (such as health information and information about religious affiliations), this exemption may be of reduced significance.

16. SERIOUS INVASIONS OF PRIVACY

16.1 In December 2024, an amendment to the Privacy Act introduced a new tort for serious invasions of privacy. This amendment will commence by 10 June 2025 (or an earlier day proclaimed by Government). Under these new provisions a person can seek injunctions, declarations, apologies and damages (amongst other things) if they can establish:

(a) there has been an invasion of privacy by either intrusion upon the person's seclusion (e.g., physical intrusion on their private space) or the misuse of information that relates to the person;

(b) the person has a reasonable expectation of privacy in all of the circumstances;

(c) there was an element of fault on the part of the defendant (i.e., the invasion of privacy must have been intentional or reckless, rather than merely negligent);

(d) the invasion of privacy was serious; and

(e) the public interest in the person's privacy outweighs any countervailing public interest (such as freedom of expression or freedom of the media).

16.2 The Privacy Act provides non-exhaustive lists of factors that will guide courts in their assessment of reasonable expectations of privacy and the 'seriousness' of the invasion of privacy.

16.3 It is a defence to the cause of action if the defendant's conduct was required or authorised by law; the defendant reasonably believed the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person; the plaintiff impliedly or expressly consented to the invasion of privacy; or the invasion of privacy was incidental to the exercise of a lawful right of defence of persons or property and proportionate, necessary and reasonable. There are also defences similar to those in defamation law, including absolute privilege, publication of public documents, and fair report of proceedings of public concern. There are also other defences that are likely to be less relevant to Schools.

16.4 The plaintiff must be an individual. However, the defendant does not need to be an 'APP entity' (i.e., any individual or organisation, including an alumni organisation, can be sued under this tort).

17. DOXXING

17.1 In December 2024, the *Privacy and Other Legislation Amendment Act 2024* (Cth) made 'doxxing' a criminal offence by amending the Criminal Code Act 1995 (Cth). While it is unlikely that this will affect Schools themselves, they should be aware that press reports indicate that School students may engage in this practice.

17.2 Doxxing is the use of a carriage service to make available, publish or distribute personal data (i.e. information about an individual that enables them to be identified, contacted or located), where the person engages in the conduct in a way that reasonable persons would regard as being menacing or harassing. This offence will be punishable by up to 6 years' imprisonment.

17.3 The Act also creates a separate doxxing offence where the personal data subject to the doxxing is of one or more members of a group and the offender engages in the doxxing in whole or part because of the offender's belief that the group is distinguished by their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin. This offence is punishable by up to 7 years' imprisonment.

18. ARTIFICIAL INTELLIGENCE (AI)

18.1 Where Schools handle personal information in connection with AI tools and AI systems (AI systems), for example to assist in their operations and teaching and learning, they must comply with their privacy obligations. Use of personal information in connection with an AI system may pose serious privacy risks and schools may wish to consider seeking specific advice and implementing appropriate AI governance measures before an AI system is adopted for use. This section of the Manual provides a high level overview of some of the privacy compliance obligations associated with AI systems.

18.2 Privacy obligations apply to personal information:

18.2.1 collected by, or for use in, an AI system;

18.2.2 disclosed or input into AI systems, including to train or fine-tune the AI system; or

18.2.3 generated or inferred by an AI system.

(i) only collecting personal information that is reasonably necessary for the School's functions or activities;

(ii) obtaining individuals' consent to collect sensitive information;

(iii) only collecting personal information by lawful and fair means; and

(iv) collecting personal information about an individual only from that individual, unless it is unreasonable or impracticable to do so;

18.3.4 the use and disclosure (including cross-border disclosure) of personal information (APPs 6 and 8 and potentially other APPs depending on the type of information and the purpose of use/disclosure). This includes:

(i) only using and disclosing personal information for a purpose that is permitted under APP 6. Any use of personal information by an AI system must only be for the primary purpose for which it was collected, unless the School has informed consent or can establish the secondary use would be reasonably expected by the individual and is related (or directly related, for sensitive information) to the primary purpose. The secondary use may be within the individual's reasonable expectations if it was expressly outlined in a notice at the time of collection and in a School's privacy policy. Given the significant privacy risks presented by AI systems, it may be difficult to establish reasonable expectations for an intended use (and/or disclosure) of personal information for a secondary AI-purpose without clear prior notification. To avoid the risk, Schools could consider seeking consent and/or offering individuals a meaningful and informed ability to opt-out; and

(ii) taking steps to ensure any cross-border disclosure of personal information complies with APP 8 (e.g., taking reasonable steps to ensure the recipient does not breach the APPs);

18.3.5 the quality of personal information (APP 10), including the quality of personal information inputted into the AI system and generated from the AI system; and

18.3.6 the security of personal information (APP 11).

18.4 OAIC guidance

The OAIC has published guidance that Schools should consider before procuring an AI system and handling personal information in connection with the AI system. There is separate guidance on:

18.4.1. the use of commercially available AI products; and

18.4.2. developing and training generative AI models (including when a School fine-tunes an AI product).

The guidance is available on the OAIC's website.

18.5 Tip for privacy compliance when using AI systems

- Establish AI governance, policies and procedures. This should include clearly defining permitted AI systems and the permitted use of those systems and what, if any, personal information can be used in relation to those systems.
- Conduct staff AI literacy training, including on the School's general AI policies and procedures, as well as specific AI systems that are approved for use by the School.
- Provide clear workplace directions to School personnel, including about how AI can and cannot be used.
- Where possible, use de-identified information, rather than personal information, in connection with AI systems.
- Do not input personal information into publicly available AI systems, as a matter of best practice, due to the significant privacy risks involved, without seeking specific advice.
- Consider conducting a privacy impact assessment for each AI system proposed to be used by the School (where personal information is either input into, or generated by, the AI system) during the procurement stage. At a minimum, the School should have a detailed understanding of the personal information flows associated with the AI system, including personal information collection (including generation), use, disclosure (including cross-border disclosure), access, storage and deletion. Each information flow should be assessed to ensure the School has taken steps for compliance with the relevant APP for that information flow.
- Conduct due diligence on any AI system the School is considering using, including whether it has been tested and proven for the School's use case.
- Where consent is needed, consider whether students have capacity to consent to privacy decisions relevant to the handling of personal information by the AI system, and otherwise seek substituted consent (capacity is considered in Section 7 of Part C of this Manual (Consent and Young People));
- If a provider of an AI system will store, have access to or otherwise handle any personal information:
  - » conduct due diligence on the provider;
  - » consider whether the provider collects data from publicly available sources to train the AI system and the privacy compliance and reputational implications of this;
  - » ensure the contract with the provider contains appropriate privacy protections and warranties (including preventing the provider from using any personal information for other purposes, such as training other products); and
  - » if personal information will be disclosed to the provider outside Australia, ensure any necessary steps are taken to comply with APP 8.
- Update privacy notifications (privacy policies and collection notices) to clearly explain the School's handling of personal information in connection with AI systems (including any cross border disclosures). Depending on how an AI system is being used, Schools may need to provide a specific, detailed, privacy collection notice for their use of AI systems, in addition to addressing their use of AI systems in their general privacy collection notices.
- Establish procedures for explaining AI-related decisions and outputs to affected individuals.
- Ensure AI systems have human oversight and that reasonable steps are taken to verify any personal information generated by AI systems.
- Audit staff use of AI systems.
- Appropriately label AI generated content to promote transparency.

19. EU GENERAL DATA PROTECTION REGULATION

Introduction

19.1 The European Union (**EU**) General Data Protection Regulation (**GDPR**) came into force on 25 May 2018. The GDPR harmonised data privacy laws across Europe and applies directly in all countries that are members of the EU. It is relevant in Australia due to the potential extra-territorial reach to Australian organisations.

Application of the GDPR to Schools

19.2 The GDPR will apply to an Australian organisation (including a School) if they:

(a) have an 'establishment' (e.g., the effective and real exercise of activity through stable arrangements) in the EU (regardless of whether or not they collect and process personal information in the EU); or

(b) do not have an establishment in the EU, but either:

(i) offer goods or services (e.g., advertise or offer education by recruiting EU students) to individuals in the EU (regardless of whether payment is required); or

(ii) monitor the behaviour of individuals in the EU (e.g., profiles them when they visit the organisation's website).[7]

The GDPR may also apply to a School through a contract it enters into with a party that is subject to the GDPR and wishes to pass on privacy related obligations to the School that it is required to under the GDPR. This may include an EU based third party service provider or an agent the School uses in the EU. Legal advice should be sought in relation to what terms should be agreed and Schools should not automatically agree to be bound by any GDPR contractual obligations.

How to comply

19.3 Guidance on compliance with the GDPR is beyond the scope of this Manual. However Schools should note that while there are some key differences, compliance with the APPs (as interpreted by the OAIC in its APP Guidelines) will broadly support compliance with the GDPR because the GDPR and APPs both:

(a) implement a privacy by design approach to compliance;

(b) focus on transparency in information handling practices; and

(c) require compliance with a set of privacy principles.

19.4 The key differences between the APPs and the GDPR relate in particular to additional rights individuals have under the GDPR, such as the right to be forgotten, the high threshold for valid consent and the right to request that personal information is not processed further. Legal advice should be sought where necessary.

Further information

19.5 The OAIC has published resources which aim to help Australian organisations understand the requirements in the GDPR and how they can comply with the GDPR and Australian privacy laws. These are available on the OAIC website.[8]

19.6 Schools should seek legal advice if they are unsure if the GDPR applies to them directly or through its extra-territorial application or through a contract and what, if any, obligations they have under the GDPR.

[7] Article 3.

[8] https://www.oaic.gov.au/privacy/guidance-and-advice, in particular https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation

PART D

Explanation of APPs as they apply to Schools

This Part sets out a detailed commentary on each of the APPs. A summary of the obligations under the APPs which can be used as a checklist is contained at Section 2 of Part A of this Manual.

1. Open and transparent management of personal information (APP 1)

How to comply

Consent

Privacy Policy (APP 1.3-1.6)

How to comply

Training staff

Do's and Don'ts.

2. Anonymity and Pseudonymity (APP 2)

Comment

How to comply

3. Collection (APP 3, 4, and 5)

Basic principles of collection

Only collect personal information if it is reasonably necessary for the School's functions or activities (APP 3.2 and 3.3)

Comment

How to comply

Only collect personal information by lawful and fair means (APP 3.5)

Comment

How to comply

Only collect personal information directly from the individual, unless this is unreasonable or impracticable (APP 3.6)

Comment

Direct collections from individuals – Table 2A

Indirect collection by Schools (i.e. collection from someone other than the individual) – Table 2B

How to comply

Ensure individuals are aware that their personal information is being collected and why (APP 5)

Comment

How to comply

NAPLAN Notices

Standard Collection Notice

Alumni Collection Notice.

Employment Collection Notice (for job applicants)

Contractor/Volunteer Collection Notice

Only collect sensitive information with consent, unless an exception applies (APP 3.3 and 3.4)

Collecting sensitive information with consent

Collecting sensitive information without consent

How to comply

If a School receives unsolicited personal information, consider whether it should be retained or destroyed (APP 4)

Collection through surveillance

Summary of collection requirements

Collection Compliance Steps – Table 3A

Personal information (excluding sensitive information) collection – Table 3B

Sensitive information collection – Table 3C

Do's and Don'ts.

Additional Do's and Don'ts for sensitive information

4. Use and disclosure of personal information (APP 6)

Primary and related purpose

Use and disclosure of information about students – Table 4A

Use and disclosure of information about parents – Table 4B

Use and disclosure of information about contractors – Table 4C

How to comply

Use or disclosure required by law (APP 6.2(b))

How to comply

Use and disclosure compliance steps – Table 4D

Do's and Don'ts.

5. Direct Marketing (APP 7)

Comment

How to comply

6. Cross-Border Disclosure of personal information (APP 8)

How to comply

7. Adoption of government related identifiers (APP 9)

Comment

How to comply

Do's and Don'ts.

8. Data Quality (APP 10)

Comment

How to comply

Sharing personal information

Do's and Don'ts.

9. Data security (APP 11)

Typical areas of concern

Reasonable steps

How to comply

Use of the Internet and emails137

Destruction and permanent de-identification (APP 11.2)

Comment

How to comply

Do's and Don'ts.

10. Access (APP 12)

Comment

Unreasonable impact on the privacy of others

Frivolous or vexatious requests

Access would be unlawful or denial of access is required or authorised by law

How to comply

Giving access by other means

Time periods

Particular issues

Do's and Don'ts

11. Correction

Comment

How to comply

Do's and Don'ts.

1. OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION (APP 1)

1.1 Requirement:

The object of this principle is to ensure that a School manages personal information in an open and transparent way (APP 1.1).

1.2 Requirement:

A School must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the School's functions or activities that:

(a) will ensure that the School complies with the APPs and a registered APP code (if any) that binds the School; and

(b) will enable the School to deal with inquiries or complaints from individuals about its compliance with the APPs or such a code (APP 1.2).

1.3 The Privacy Act has an overriding object, which is that APP Entities must manage personal information in an open and transparent way. To achieve this objective, a School must plan in advance how it will handle personal information before it collects and processes it.

1.4 This requires the School to plan in advance how to:

(a) comply with each of the APPs;

(b) respond to complaints and inquiries about its compliance with the APPs; and

(c) take 'such steps that are reasonable in the circumstances' to implement practices, procedures and systems relating to its functions and activities to achieve this.

1.5 **Reasonable steps**: what steps are reasonable for a School to take will depend upon all the circumstances, which may include:

(a) the nature and volume of the personal information held (more rigorous steps may be required as the amount and sensitivity of personal information handled increases);

(b) the possible adverse consequences for an individual if their personal information is not handled according to the APPs;

(c) the nature of the School (e.g., the School's size and resources and whether the School gives database and network access to contractors which may require additional safeguards); and

(d) the practicability, including time and cost involved. However, a School is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so.[9]

1.6 As part of complying with the APPs, a School will also be required to consider privacy obligations when planning any new systems. This is part of the move to a 'privacy by design' approach to compliance reflected in APP1 - that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception.

1.7 The significance of this principle is three-fold:

(a) this is an overarching requirement;

(b) the OAIC has the power to investigate whether a School is properly managing personal information, even where there has been no breach of an APP or complaint; and

(c) if a School is found to be in breach of another APP, it is quite possible that it will also be found to be in breach of APP 1.

How to comply

1.8 The School:

(a) is required to plan in advance how it will handle personal information in compliance with the APPs prior to collecting and processing any personal information;

(b) should train and communicate to staff information about the School's information handling policies and practices;

[9]APP Guidelines 1.6, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

(c) should establish procedures to receive and respond to requests for access and correction, complaints and other inquiries;

(d) should develop information to explain its policies and procedures; and

(e) should establish procedures to identify and manage privacy risks and compliance issues, including in designing and implementing systems or infrastructure for the collection and handling of personal information by the School.

1.9 As part of the School's practices, procedures and systems it must implement to ensure compliance with the APPs, the School should consider appointing a privacy officer (depending on the size of the School). A privacy officer can be the first point of contact for internal and external queries on privacy matters and coordinates a School's privacy compliance. They may also conduct privacy training, The privacy officer does not need to be the only role that a staff member has, this role can be allocated to an existing staff member having regard to their other role and experience. The School's privacy policy should provide the contact information of the privacy officer. For this purpose, and given changing staff roles, a generic contact is sufficient (such as the School's general phone number and a dedicated email address e.g., privacy@[School's email address]). If it is not possible to include the privacy officer's contact details, the privacy policy should contain the Principal's contact details or, at the very least, the general contact details for the School. Everyone at the School should be made aware who the privacy officer is.

1.10 Attached at Annexure 4 are Privacy Planning Templates intended to assist a School in assessing the personal information that it currently collects and identifying risks involved.

Consent

1.11 Throughout the APPs there are obligations which require consent to be obtained from individuals. It is part of being open and transparent that consent is freely obtained and is not hidden in lengthy documents or as part of multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information. Individuals should have the opportunity to choose which collections, uses and disclosures they consent to (where consent is required). The practice of obtaining bundled consents has the potential to undermine the voluntary nature of a consent.

Privacy Policy (APP 1.3-1.6)

1.12 Requirement:

A School must have a clearly expressed and up-to-date policy about the management of personal information by the School (APP 1.3).

1.13 Requirement:

The Privacy Policy of a School must contain the following information:

(a) the kinds of information it collects and holds;

(b) how it collects and holds information;

(c) the purposes for which it collects, holds, uses and discloses information;

(d) how an individual may access and seek correction of their information;

(e) how an individual may complain about a breach of the APPs and how the School will deal with that complaint; and

(f) whether the School is likely to disclose information overseas and, if so, the countries in which the recipients are likely to be located (if practicable to specify) (APP 1.4); and

(g) in addition, from 10 December 2026, the Privacy Policy of a School must contain specified information about the School's use of personal information in connection with any automated decision making the school undertakes (see paragraph 1.2B of Part C) .

1.14 Requirement:

A School must take such steps as are reasonable in the circumstances to make its Privacy Policy available free of charge, and in such form as is appropriate. A School will usually make its Privacy Policy available on its website. (APP 1.5).

1.15 Requirement:

If a person requests a copy of the Privacy Policy in a particular form, the School must take such steps as are reasonable in the circumstances to give the person or body a copy in that form. (APP 1.6).

1.16 It is important that a Privacy Policy (or similar document) be made widely available (including to employees and contractors).

1.17 In addition, it is important that where policies are in place (e.g., policies in respect of confidentiality or Internet and email usage) that these policies are adequately enforced.

How to comply

1.18 Adopt a Privacy Policy which expresses, in plain language, the School's policy or policies on its management of personal information. An 'up-to-date' Privacy Policy should be one that is a 'living document' and is reviewed regularly. It would be sensible to diarise a review at least once every 12 months. The APP Guidelines provide that, '*at a minimum, a clearly expressed policy should be easy to understand (avoiding jargon, legalistic and in- house terms), easy to navigate, and only include information that is relevant to the management of personal information by the entity*'.

1.19 Draft a Privacy Policy (an example is at Annexure 5) which covers the following issues:

(a) the kinds of personal information the School collects and how it collects this information;

(b) the purpose of collection;

(c) how any why personal information is used, shared and disclosed;

(d) the use of personal information as part of automated decision making;

(e) access and correction of information;

(f) direct marketing;

(g) the disclosure of information overseas (including listing countries if practicable to specify);

(h) storage and management of information;

(i) any exemptions in the Privacy Act that apply; and

(j) complaints.

1.20 The example Privacy Policy at Annexure 5 is intended to comply with APP 1 and can be adapted as required by the School. Not only can this Privacy Policy be used to help inform individuals about the practices of the School in relation to personal information, but it can also serve as a guide to the School's staff as to the standard to be applied in respect of handling personal information and ensure consistency in the School's approach to information privacy.

1.21 Make the Privacy Policy available on the School's website and draw attention to it when collecting personal information (i.e. by referring to it in a privacy collection notice).

Training staff

1.22 The key to achieving compliance and ensuring continued compliance with the Privacy Act will be through the conduct of the School's employees and other staff members. Consequently, the School's staff members must be trained in the principal requirements of the Privacy Act.

1.23 There are a number of ways that employees and other staff members should be made aware of the requirements of APP 1 (and the other obligations under the Privacy Act). These include raising general awareness by:

(a) circulating the Privacy Policy to all staff and requiring them to acknowledge they have read it;

(b) informing staff of the requirements of confidentiality and extending this obligation contractually where necessary;

(c) holding internal seminars and workshops; and

(d) frequently reminding staff of their privacy obligations in staff meetings or similar (e.g. in a staff meeting at the beginning of each term staff could be verbally reminded of a particular obligation of relevance to them).

Do's and Don'ts

DO ensure the School has practices, procedures and systems that will ensure compliance with the APPs and enable the School to deal with inquiries or complaints. Regularly review and test these practices, procedures and systems.

DO, if asked, inform people about the type of personal information that is being collected about them and why.

DO require staff members to read the School's Privacy Policy and encourage them to do this on an annual basis.

DO make the Privacy Policy easily accessible.

DO ensure that the School's requirements in relation to collection, use and disclosure of personal information are followed.

DO include contact details for the School's privacy officer (if any) in the Privacy Policy (such as the School's general phone number and a dedicated email address such as privacy@[School's email address]) and ensure staff refer all queries about the Privacy Policy to the School's privacy officer.

DO conduct staff privacy training.

2. ANONYMITY AND PSEUDONYMITY (APP 2)

2.1 Requirement:

Individuals must have the option of not identifying themselves or using a pseudonym when dealing with a School unless:

(a) the School is required or authorised by law to deal with individuals who have identified themselves; or

(b) it is impractical to deal with individuals who have not identified themselves.

Comment

2.2 The OAIC considers that unless there is a good practical or legal reason to require identification, a School must give people the option to interact anonymously.

2.3 Anonymity is an important element of privacy. However, in some circumstances, it will not be practicable to do business anonymously. In others there will be legal obligations that require identification of the individual. This principle is not intended to facilitate illegal activity.

How to comply

2.4 It is likely that APP 2 will be of little significance to most Schools as they would usually need to know the identity of most people with whom they deal.

2.5 However, APP 2 may apply where:

(a) a prospective parent makes an enquiry about the School over the phone; or

(b) a School receives a complaint and the complaint is given anonymously in accordance with a whistle blower policy. Schools should consider whether their collection processes for complaints need to incorporate the ability to receive complaints anonymously to address situations involving whistleblowing, particularly if the School is subject to whistleblowing legislation. This should be consistent with the School's whistleblowing policy (if any).

3. COLLECTION (APP 3, 4, AND 5)

Basic principles of collection

3.1 There are six basic principles to follow when collecting personal information. They are:

(a) only collect personal information if it is **reasonably necessary** for the School's functions or activities (see Paragraph 3.4);

(b) only collect personal information by **lawful and fair means** (see Paragraph 3.10);

(c) only collect personal information **directly from the individual**, unless this is unreasonable or impracticable (see Paragraph 3.16);

(d) ensure individuals are **aware** that their personal information is being collected and why (see Paragraph 3.25);

(e) only collect **sensitive information with consent**, unless an exception applies (see Paragraph 3.57); and

(f) if a School receives **unsolicited personal information**, consider whether it should be **retained or destroyed** (see Paragraph 3.73).

3.2 The first five principles only apply to solicited information. 'Solicited' personal information is personal information that the School has asked the individual or a third party to provide (or to provide a kind of information in which that information is included). All other personal information is 'unsolicited'.

3.3 Each of the principles above is considered in detail in this Section, from Paragraphs 3.4 to 3.75. The remainder of this Section contains:

(a) guidance on collection through surveillance (see Paragraph 3.76);

(b) a flow chart and tables summarising the collection requirements (see Paragraph 3.80); and

(c) collection do's and don'ts.

Only collect personal information if it is reasonably necessary for the School's functions or activities (APP 3.2 and 3.3)

3.4 Requirement:

A School must not collect solicited personal information (including sensitive information) unless the information is reasonably necessary for one or more of its functions or activities (APP 3.2 and 3.3).

Comment

3.5 The OAIC interprets 'reasonably necessary' in a practical sense: the APP Guidelines provide that it is an objective test, namely, 'whether a reasonable person who is properly informed would agree that the collection is necessary'. The APP Guidelines state that 'the test must be applied in a practical sense': if a School cannot effectively pursue a legitimate function or activity without collecting personal information, then ordinarily such collection would be deemed to be 'necessary' for one or more of its functions or activities. However, a collection will not usually be considered reasonably necessary if there are reasonable alternatives available, for example, if de-identified information can be collected and used instead. A School should not collect information on the 'off-chance' that it will be of some use in the future.

3.6 The collection of personal information which is required by law would be deemed as being 'necessary' for one or more of a School's functions or activities.

How to comply

3.7 Ensure the School is aware of all kinds of personal information, including sensitive information, collected by the School. These should be listed in the School's privacy policy.

3.8 Ensure that all kinds of personal information identified as being collected are reviewed as to whether their collection is necessary for one or more of the School's functions or activities.

3.9 The Personal Information Planning Templates at Annexure 4 are intended to assist Schools in identifying and determining how to deal with personal information that it collects.

Only collect personal information by lawful and fair means (APP 3.5)

3.10 Requirement: A School must collect personal information:

(a) only by lawful and fair means; and

(b) not in an unreasonably intrusive way.

Comment

3.11 Under the APP Guidelines, a 'fair' means of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive. What is fair will depend on the circumstances. For example, covert collection will usually be considered as unfair collection. However, this may be a fair means of collection if undertaken in connection with an investigation into fraud or serious misconduct.

3.12 Examples of what might be considered unfair or unreasonably intrusive ways of collection include:

(a) calling an individual late at night or at meal time without a prior arrangement to do so;

(b) asking for information for one purpose when really it is for another purpose;

(c) misrepresenting the consequences for the individual of not providing the information;

(d) telling an individual that it is compulsory that they provide personal information when it is not;

(e) asking for sensitive personal details within earshot of other people;

(f) collecting from an electronic device which is lost or left unattended;

(g) collecting from an individual who is traumatised, in a state of shock or intoxicated; and

(h) collecting in a way that disrespects cultural differences.

How to comply

3.13 The School should regularly review its collection procedures and particular acts and practices of collection should be identified and monitored for instances (whether systemic or by particular individuals) of unfair, unlawful or unreasonably intrusive collections.

3.14 Any complaints concerning the methods of collection should be part of this monitoring process.

3.15 The School should be careful to consider and re-consider the context in which personal information is collected and should always be mindful that personal information and sensitive information should be collected discretely where possible.

Only collect personal information directly from the individual, unless this is unreasonable or impracticable (APP 3.6)

3.16 Requirement:

If reasonable and practicable, personal information must only be collected directly from the individual.

Comment

3.17 APP 3.6 aims to ensure that where it is reasonable and practicable to do so a School will collect information about an individual only from that individual.

3.18 In the case of Schools this is often not practicable. For example, personal information of young students is frequently collected from their parents on the basis that it would be impracticable to obtain this from the young students (who do not themselves know the information, or may provide incorrect information).

3.19 Personal information is collected by Schools in a number of different ways. The following table indicates some ways of direct collections (assuming the information is collected by the School for inclusion in a record or a generally available publication, rather than merely heard by a staff member and not recorded).

Direct collections from individuals – Table 2A

Collection point	Collection method (& source)
Direct contact	• employment interviews (employees and job applicants) • meetings (e.g., P&F) (from parents) • face-to-face contact with students, staff members and parents • writing (e.g., letters from parents)
Forms and Documentation	• enrolments forms (parents) • medical forms (parents) • various other forms concerning students, staff members and parents • emails and Internet • resume
Telephone	Calls received from: • parents • staff members • others

3.20 The following indicates some instances of indirect collection by Schools (ie when an individual's personal information is collected from someone else). It is also necessary to consider the section on receipt of unsolicited personal information at Paragraph 3.72 of Part D of this Manual.

Indirect collection by Schools (i.e. collection from someone other than the individual) – Table 2B

Individual concerned	Third party source of collection
Students of another school	• Principal of another school
Students	• Professionals (e.g., counsellors, doctors, speech pathologists, therapists, other agencies) through reports and general information (e.g., medical, vision, hearing, speech tests) and other results (e.g., psychometric) • Parents and staff in performance appraisals
Students	• CEC (or equivalent in your State or Territory, e.g., CSNSW) and AIS
Students	• Parent through various forms (e.g., enrolment form, medical advice form, deed of indemnity)
Students	• Government welfare agencies/departments (regarding safety of child at home)
Students	• Parent (and vice versa)
Students and staff members	• Students and/or staff members through various forms (e.g., incident report, Child Protection Notification Form) • Students who name them to counsellors or staff members during counselling or advising or in an incident report
Students and parents	• Priests (reference) • Previous school (reference)
Students or prospective students in New South Wales	• Another school for the purpose of assessing whether the enrolment of the student or prospective student would pose a risk to the health or safety of any person and to develop and maintain strategies to eliminate or minimise that risk*
Parents	• Other parents or others (e.g., P&F, development office for fundraising) • Medical practitioners (e.g., mother has cancer) • School (e.g., in Student Report Card)

Indirect collection by Schools (i.e. collection from someone other than the individual) – Table 2B

Individual concerned	Third party source of collection
Students' family members	• Student (e.g., pray for sick parent or Grandparent)
Employees and Contractors	• Referees who provide information upon request
Previous employers	• Staff members and job applicants through various forms (e.g., application form) and resume
Job applicants	• Previous employers • Police through criminal record checks
Spouses of job applicants	• Job applicants through provision of marriage certificate.
Contractors	• Dun & Bradstreet due diligence searches
Referees	• Staff members and job applicants through various forms
Next of kin	• Students, staff members and parents through various forms (e.g., enrolment form)
Emergency contacts	• Students, staff members and parents through various forms (e.g., enrolment form, staff detail form)
Nominated siblings/ family members	• Students and parents through various forms (e.g., enrolment form)
Doctor	• Parent (e.g., from enrolment form, student information sheet)
Others	• Photographs

*Please refer to Section 11 of Part C of this Manual for more information.

3.21 It is apparent that it will not always be reasonable and practicable to collect personal information from the individual directly. In most scenarios, the individual concerned is aware of this indirect collection and it is permitted as it is unreasonable or impracticable to collect the information directly from the individual. However, this may not always be the case.

3.22 Where a school needs a detailed reference from a previous employer or other referee it will clearly be impracticable to obtain this from the job applicant. However, in order to comply with APP 5, the applicant should be told that this information is being collected. Schools should note however that 'collection' only relates to information that is contained in a record. Information obtained from an inquiry which is not recorded does not constitute a record and therefore no collection occurs.

How to comply

3.23 Before collecting personal information about an individual from a third party (including a parent), confirm it is unreasonable or impracticable to collect the information directly from the individual.

3.24 There may be some circumstances in which information should only be collected directly from the individual (even if this is considered impracticable). These circumstances should be considered on a case by case basis.

Example:

Where it is likely that the information is incorrect (e.g., the source is unreliable) then the School collecting the information should endeavour to contact the individual concerned to check whether the information is accurate. It will not always be reasonable and practicable to do this. For example, the individual concerned may be the subject of an allegation about an unlawful activity and approaching that person may prejudice the investigation.

Ensure individuals are aware that their personal information is being collected and why (APP 5)

3.25 Requirements:

At or before the time (or, if not practicable, as soon as practicable after) a School collects personal information about an individual from the individual, the School must take such steps (if any) as are reasonable in the circumstances to notify or make the individual aware of such of the following matters that are reasonable in the circumstances:

(a) the School's identity and contact details;

(b) if the individual may not be aware that the information has been collected or if the School collected the information from a third party, the fact that it has been collected and the circumstances of the collection;

(c) if collected under or authorised by law, the fact that the collection is so required or authorised (including details of the law requiring or authorising collection);

(d) the purposes for which it is collected;

(e) the main consequences if it is not collected;

(f) any other entities or types of entities to whom the information may be disclosed;

(g) that the Privacy Policy contains information about how an individual can access and seek correction of information;

(h) that the Privacy Policy sets out how complaints may be made, how an individual may complain about a breach of their privacy and how the complaint may be dealt with; and

(i) whether information is likely to be disclosed overseas and, if so, to which countries, if practicable to specify.

Comment

3.26 Deciding on whether a School should make individuals aware of the required matters 'at or before the time of collection' will depend on the circumstances. This can be done after collection of the information if there are practical problems in doing so before collection.

3.27 APP 5.1 has a 'double reasonableness' provision. A School is only required to take 'reasonable steps' to inform people of such of the required matters that are 'reasonable' in the circumstances. Therefore it is recognised that where such of those matters are obvious, irrelevant or can be easily located (e.g., the identity of the School) it may not be necessary to inform people of that matter in a collection statement. The APP Guidelines provide that it is the responsibility of the entity to be able to justify not taking any steps.

3.28 In the same way, where the circumstances of collection make a matter listed in APP 5.1 obvious, then the 'reasonable steps' might not involve any active measures because the circumstances speak for themselves. For example, if the matters contained in APP 5.1 were made available to an individual for a certain type of collection, then the same collection later may not require that the APP 5.1 matters (if unchanged) be repeated to the individual.

3.29 Deciding what are reasonable steps and what are matters which are reasonable to include involves balancing a number of possible factors, including the importance to the individual of having the relevant knowledge and the time and cost to the School in providing that information.

3.30 The description of the purposes can be reasonably general as long as the description is adequate to ensure that the individual is aware of what is going to be done with their personal information. Internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information do not have to be described.

3.31 Taking 'reasonable steps' to inform an individual about usual disclosures would ordinarily mean either giving general descriptions of sets of people and entities to whom the information may be disclosed (for example, State Government educational authorities and other schools) or listing each member of the set.

3.32 A School does not need to mention disclosures that the APPs permit, but in practice happen only rarely.

3.33 Reasonable steps must be taken to tell the individual about any law that requires the individual to provide, or the School to collect, personal information in the particular situation. In describing the law, the School need not specify the exact piece of legislation (although it would be desirable to do this where possible). A statement like '*The New South Wales Education Act requires us to collect this*' would ordinarily be adequate.

3.34 A School need not describe all possible consequences of not providing personal information. Only significant (and non-obvious) consequences would need to be described.

3.35 A School is required to describe the fact that it collects personal information and the circumstances of that collection. However, this is only required when the School collects the personal information from someone other than the individual or the individual may not be aware that the School has collected the personal information. If the School collects the information directly from the individual, and the individual is aware of this collection, the School is not required to describe the fact and circumstances of collection.

How to comply

3.36 A commonsense and pragmatic approach should be taken by the School when complying with APP 5.1 and APP 5.2.

3.37 Annexure 6 contains example privacy collection notices that should be adapted as required by the School. This includes a 'standard collection notice' (for parents and students), an employment collection notice (for job applicants) and a contractor/volunteer collection notice. As the information a School requires varies over the period of a student's enrolment, it is suggested that the 'standard collection notice' be reviewed and updated (and reissued) each year.

3.38 The APPs make it clear that there will be occasions where it is reasonable not to advise people of some or all of the matters set out in APP 5.2. This would be the case, for example, when those matters are obvious or likely to be known.

3.39 Where the School collects personal information about those who have not seen any collection notices (e.g., third parties) or where the collection notices do not cover a particular situation, then the School should consider, with reference to the APPs and any available Guidelines, whether it needs to take additional steps to comply with APP 5.1 and notify those people of the matters set out in APP 5.2. In particular, where a School intends to use a film including a student or a student's photo in a public forum (such as on television or on social media, such as Facebook and Flickr) the student's and/or the student's parent's permission should be sought as appropriate. This is further considered in Section 3 of Part C of this Manual.

3.40 The 'standard collection notice', which is drafted to cover the School's usual collection practices, could be tailored to suit specific situations and should deal with the matters listed in APP 5.1 concerning how any personal and sensitive information collected from the individual about him/herself or a third party would be dealt with.

3.41 The 'standard collection notice' should be distributed with all enrolment forms (and at any other initial points of collection) and could also be placed in each student's School diary. It is suggested that the then-current notice be sent at the commencement of each school year to parents of students at the same time as other materials are sent.

3.42 The School should consider placing a 'standard collection notice' in other relevant documents (e.g., it may be appropriate to insert a modified collection notice in a form designed to collect a student's medical information).

NAPLAN Notices

3.43 All schools in Australia are required to participate in the National Assessment Program – Literary and Numeracy (**NAPLAN**). The sample 'standard collection notice' in Annexure 6 (as well as the sample privacy policy in Annexure 5) include information that reflects the personal information flows associated with NAPLAN (including the potential disclosure by Schools of parents' and students' personal information as part of NAPLAN online).

3.44 Schools will also be provided with a separate NAPLAN specific notice that Schools will need to provide to parents. This notice will need to be provided to parents each year before NAPLAN testing commences (usually as part of an information pack with general information about NAPLAN). This NAPLAN specific notice is not included this Manual.

Standard Collection Notice

3.45 Attached at Annexure 6 under the heading 'Standard Collection Notice' is suggested wording for a general collection notice for parents and students. It needs to be adapted to suit the situation of the School. The 'School' refers both to Independent Schools, and a Diocese both independently and through its Schools.

3.46 This standard collection notice will not be able to cover every situation where a School collects personal information and each School should consider (a) what types of information they usually collect and should cover and (b) whether additional collection notices need to be provided in particular situations at particular points in time. For example, a separate collection notice should be provided to VET (Vocational Education and Training) students as part of the enrolment process.

Alumni Collection Notice

3.47 At some Schools, students' personal information will be sent to the School's alumni or similar association when the student leaves the School. When this occurs, the School should insert an appropriate collection notice in a relevant form (e.g., in an Application for membership of Alumni Association form). The School should also consider whether it should obtain the student's consent. If the student is young, such as when leaving a preparatory school, it may be appropriate to seek the parent's consent to include the child's name on an Alumni register.

3.48 The School might wish to forward to the student, on behalf of the Alumni Association, relevant documentation inviting the student to join the Association (including a collection notice).

3.49 The content of the collection notice will depend on the structure of the Alumni Association and its relationship with the School.

Employment Collection Notice (for job applicants)

3.50 When receiving employment applications an 'employment collection notice' should be sent to the individual with the acknowledgment. A sample collection notice for job applicants is contained at Annexure 6 under the heading 'Employment Collection Notice'.

3.51 The employee records exemption (see Section 14 of Part C) does not apply to job applicants. Therefore, under the access and correction provisions in APP 12 and 13 (see Sections 10 and 11 of Part D of this Manual) job applicants may seek access to and correction of records of their personal information which the School holds about them. The School should be mindful of this when collecting personal information (e.g., references, making notes and reports). The APPs provide that personal information should be de-identified or destroyed when it is no longer needed. If Schools wish to retain this information on file, in case another position becomes available, this should be included in the collection notice. The same applies to contractors.

3.52 When collecting sensitive information, APP 3.3 requires that consent be obtained, unless an exception applies (such as where collection is required by law – see APP 3.4(a)). Regardless of whether consent for collection is required, APP 5 (relating to collection notices) must still be complied with. The requirement for consent when collecting sensitive information is discussed in Paragraph 3.57 of Part D.

3.53 If unsolicited job applications are received and the School wishes to retain the applicant's information, the 'employment collection notice' should be sent to them.

3.54 If you intend to pass on information to a related School, you should make the applicant aware of this in the 'employment collection notice'.

Contractor/Volunteer Collection Notice

3.55 In most circumstances, all new contractors and volunteers should be sent a modified version of the 'employment collection notice'. However, there may be circumstances when a collection notice is not needed, particularly in respect of parent volunteers (e.g. when a parent volunteers to assist in their child's classroom and the parent has previously been provided the 'Standard Collection Notice' in Annexure 6).

3.56 A sample collection notice for contractors is contained at Annexure 6 under the heading 'Contractor Collection Notice'.

Only collect sensitive information with consent, unless an exception applies (APP 3.3 and 3.4)

3.57 Requirement:

In general, a School must not collect sensitive information about an individual, unless an applicable exception applies. The definition of sensitive information is set out in Paragraph 4.4 of Part A of this Manual.

The exceptions include where:

(a) the individual has consented;

(b) collection is required by law, which includes the common law duty of care;

(c) it is unreasonable or impracticable to obtain the individual's consent to the collection and the collection is necessary to prevent or lessen a serious threat to the life or health of any individual; or

(d) other specific circumstances exist for sensitive information which is health information.

3.58 In a large number of cases, sensitive information, including health information, will be provided by the parents or students themselves, in which case it is clear that the School has consent to collect that information. On occasions, Schools may receive sensitive information from third parties in circumstances where that collection is permitted under the Privacy Act without consent. For example, one School may advise a second School about health issues relating to a student at the disclosing School who was to take part in an event at the second School, in order for the second School to exercise its duty of care. In that instance, the collection of that information by the second School would be authorised by law.

Collecting sensitive information with consent

3.59 The School would normally need clear evidence that an individual had consented to it collecting sensitive information. The APP Guidelines provide that an '*An APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.*' The provision by any individual of sensitive information would usually indicate implied consent for the collection of their sensitive information. However, in this circumstance, the School should remember it should only be used for the purpose for which it was provided or a directly related purpose that the individual would reasonably expect.

3.60 A student's sensitive information should only be collected from a parent if the student does not have capacity to consent, or the student has consented to the School collecting the sensitive information. See also Section 7 of Part C – 'Consent and Young People'.

Collecting sensitive information without consent

3.61 In most situations Schools will collect sensitive information with consent on the basis that it has been provided to them directly by the student, the parent (if the student lacks capacity to consent) or a person authorised by the student (or parent if the student lacks capacity) such as a doctor.

3.62 However occasions may arise where sensitive information is collected from third parties without consent. This is permitted where it is required or authorised under law (this includes a duty of care) or it is impracticable to obtain consent and it is reasonably necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety. For example, it may be necessary when investigating a suspected case of child abuse where there is a legal obligation to make inquiries without disclosing that there is an investigation.

How to comply

3.63 Sensitive information may be collected, among other things, if the individual consents to the collection of that information, or it is required by law. In most circumstances health information is sought to enable the School's statutory obligations to be met or to enable it to discharge its duty of care. Comments on the issue of collection of sensitive information with consent from young people are contained in Section 7 of Part C of this Manual. Consent, where needed, may be able to be given by the parent.

3.64 When collecting sensitive information, the requirements of APP 3 and APP 5 must also be met. Therefore, regardless of whether APP 3.3 requires that consent be obtained before sensitive information is collected, the School, for example, under APP 3.3(a)(ii) must ensure that the collection is reasonably necessary for one or more of its functions and activities, and under APP 5.1, take such steps (if any) as are reasonable in the circumstances to notify the individual of the matters in APP 5.2. There may be some instances where notification should not be given or is unnecessary.

3.65 Sensitive information is collected by means other than by way of forms, such as during interviews, telephone calls, meetings and medical reports (assuming the information is collected by the School for inclusion in a record or a generally available publication, rather than merely heard by a staff member and not recorded). On occasions sensitive information will be collected from third parties. To pre-empt such situations, it is important that the individual whose information is collected (e.g., job applicant, student or parent) is made aware that their sensitive information is likely to be collected, and to obtain their consent to such collection. The 'standard collection notice' in Annexure 6 notifies students and parents that health information may be collected. However, this does not obtain consent. It may be appropriate on some occasions to get specific consent and give a specific collection notice.

3.66 In some instances there is collection of sensitive information due to a legal obligation to collect such information.

Example:

Examples of collection as required by law include:

(a) immunisation records and other health information required under the public health legislation; and

(b) certain criminal record checks (e.g. as required under child protection laws in some States).

3.67 Where collection of sensitive information is required by law, APP 3.4(a) will permit the collection of sensitive information without consent. However, APP 5.1 will continue to apply and it may be necessary to inform the individual that this information is being collected.

3.68 Where practicable, sensitive information should be clearly identified as being such in any records. This practice would help ensure that the persons handling the information recognise the extra confidentiality and security that should be afforded to sensitive information.

3.69 Information about religion, racial and ethnic origin is also sensitive information. If this information is collected from the individual or a parent (if a student lacks capacity to consent) then consent can be implied. However, if this information is collected from a third party (such as a parish priest) permission should first be sought. Consent can usually be obtained from the parents on the child's behalf (see Section 7 of Part C of this Manual).

3.70 Where sensitive information is collected from a third party in a standard form (which would usually be health information about a child) it would be sensible to include in the relevant form a statement to the following effect (with a tick-box that is not pre-ticked):

> 'The child who is the subject of this information or the child's parent/ guardian (if the child is under the age of 15) has consented to its collection by the School.'

3.71 This would ensure that third party providers obtain appropriate consents. However, it may not be necessary to obtain such specific consents in all cases. This is discussed in Paragraph 3.63 of this Part D.

If a School receives unsolicited personal information, consider whether it should be retained or destroyed (APP 4)

3.72 The APPs differentiate between 'solicited' information and 'unsolicited' information. 'Solicited' personal information is personal information that the School has asked the individual or a third party to provide (or to provide a kind of information in which that information is included). All other personal information is 'unsolicited'. The following paragraphs relate to unsolicited information.

3.73 Requirement:

(a) If a School receives unsolicited information it must within a reasonable period determine whether it could have collected that information under APP 3.

(b) If it determines that it could not have collected the information under APP 3 it must, if lawful and reasonable to do so, destroy or de-identify the information.

3.74 This places an obligation on Schools to ensure that they only keep information they could have collected. That is, where any unsolicited personal information it receives is reasonably necessary for one or more of the School's functions or activities. If it is sensitive information and the person has not consented to its collection, it would need to fall within one of the exceptions referred to at Paragraph 3.57 of this Part D.

3.75 On many occasions it is likely that unsolicited personal information will be received orally. In order to meet the requirements of APP 4, Schools should adopt a rule that any notes of unsolicited personal information received orally should not be made unless it is needed and, in the case of sensitive information, an exception for collection without consent exists.

Example:

A parent advises the principal that she understands that the parents of another student were intoxicated at a party they both attended.

This is not information that is relevant to the School's operations and should not be collected (i.e. written down or otherwise recorded).

Example:

A parent advises the School that a student who is a good friend of their son's is showing considerable signs of distress following his mother's serious illness (of which the School was unaware) and requires special attention.

This is relevant to the School's operations and its exercise of its duty of care and would be relevant to send in a note to the boy's teachers even though it contained sensitive information about the mother and the student. In the circumstances, it is also reasonable to take no steps to inform the mother or student of the collection of the information.

Collection through surveillance

3.76 If a School has implemented surveillance systems, including CCTV or monitoring of computer systems, networks and facilities, people interacting with the School or using those systems should be advised that they may be monitored. If a person is being monitored, even through their computer use, personal information may be collected.

3.77 Specific legislation in certain States and Territories governs the surveillance and monitoring of persons on School grounds including students, volunteers, teachers, employees and contractors. For example:

(a) in New South Wales, specific legislation requires employers to notify their employees in advance that their computer use will be monitored;

(b) additionally, legislation in New South Wales, Queensland, Victoria and Western Australia, requires employers who use surveillance devices such as security cameras, CCTV or telephone monitoring to obtain the express or implied consent of those persons to do so. This consent could be obtained via a contract of employment, through School policies or notices, or by using signs in areas where such surveillance occurs.

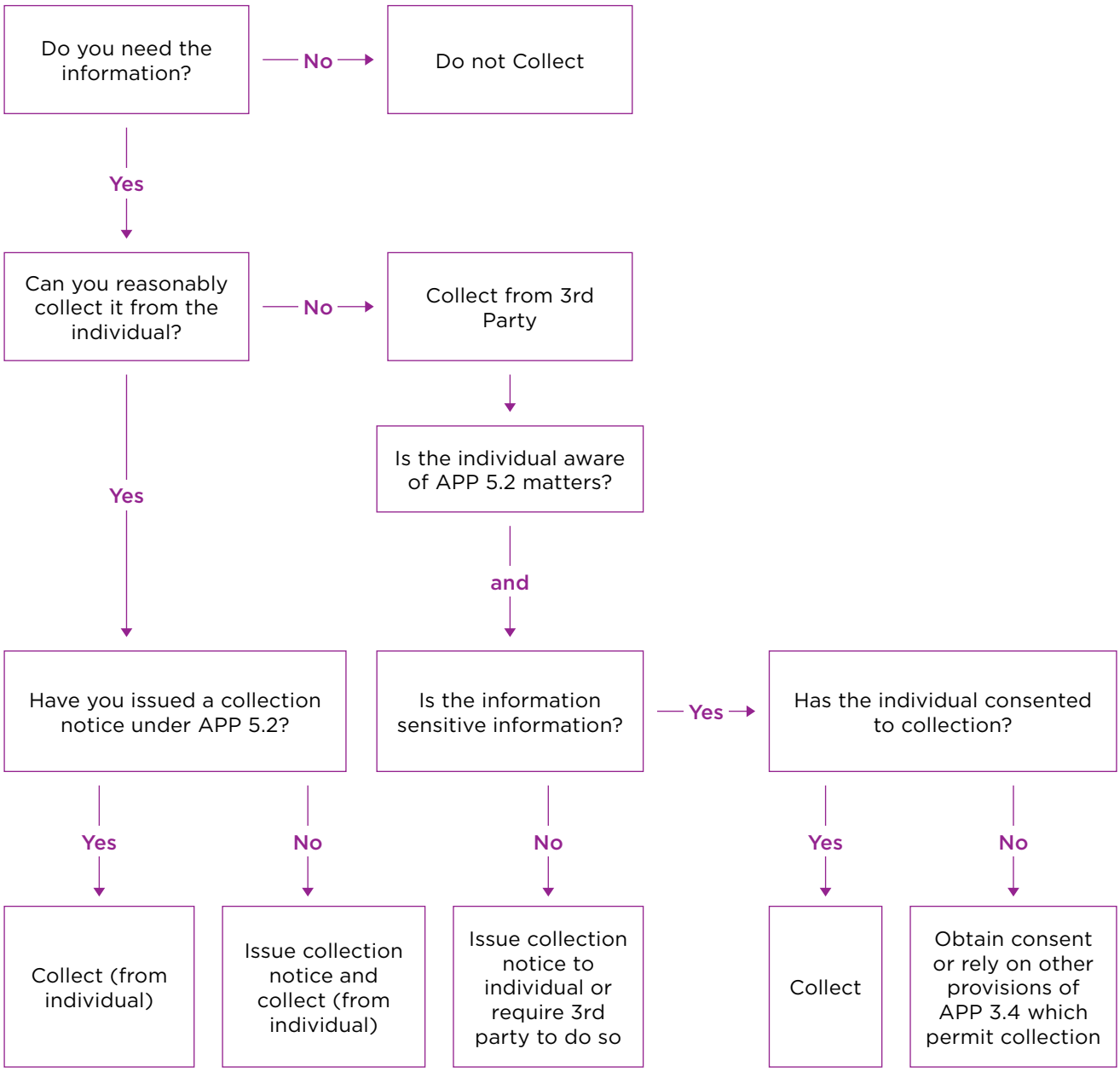
3.78 Students, volunteers, teachers, employees and contractors should be provided with a computer usage policy, noting that computer use may be monitored. Ideally, written acknowledgement that they have read that policy should be given to the school.

Additionally, students, volunteers, teachers, employees and contractors should be notified of any other instances of surveillance in the contract of employment, through School policies or notices, and/or through the use of signage in areas where a School engages in surveillance.

Summary of collection requirements

3.80 Tables 3A, 3B and 3C below illustrate the steps to be followed by the School in deciding whether it can collect personal and sensitive information.

Collection compliance steps – Table 3A



Personal information (excluding sensitive information) collection – Table 3B

Collection	Provider	Consent	Collection Notice (see e.g., Annexure 6)
Personal information about Student	Student	Not required	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
	Parent (assuming unreasonable or impracticable to collect from student)	Not required	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
	Third party (e.g., principal of another School (assuming unreasonable or impracticable to collect from student)	Not required	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice*
Personal information about parent	Parent Student (assuming unreasonable or impracticable to collect from parent)	Not required Not required	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice **or** consider if failure to notify permitted because of duty of care to student
	Third party (e.g., another parent) (assuming unreasonable or impracticable to collect from parent)	Not required	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
Personal information about Employee **	Employee or Third party	Not required	Employees should be provided with an employee collection notice (which could be included with onboarding documents)
Personal information about Contractor / Third party	Contractor / Third party	Not required	Collection notice should be given unless obvious

*__Note__: In New South Wales, collection of personal information about students and prospective students will be permitted without consent for the purposes of assisting the Director–General or other schools:

(a) to assess whether the enrolment of a particular student would pose a risk (because of the behaviour of the student) to the health or safety of any person (including the student); and

(b) to develop and maintain strategies to eliminate or minimise that risk.

** __Note__: In New South Wales information about employees and prospective employees may be able to be obtained under the *Children and Young Persons (Care and Protection) Act.*

Sensitive information collection – Table 3C

Collection	Provider	Consent	Collection Notice (see e.g., Annexure 6)
Sensitive information about Student	Student	Consent implied	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
	Parent	Consent implied, provided the student lacks capacity to consent. Otherwise, consent should be obtained from student.	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
	Third party (e.g., doctor, principal of another School)	Parent to consent on behalf of student if student lacks capacity to consent. Otherwise, consent should be obtained from student.	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
Sensitive information about parent	Parent	Consent implied	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
	Student	Consent could be implied in some circumstances, but not always. Where consent cannot be implied, seek express consent from parent.	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice **or** consider if failure to notify permitted because of duty of care to student

Collection	Provider	Consent	Collection Notice (see e.g., Annexure 6)
Sensitive information about parent	Third party (e.g., another parent)	Unlikely that consent can be implied. Where consent cannot be implied, seek express consent from parent. If information is unsolicited, consider requirements in APP 4.	Consider if covered by 'standard collection notice', otherwise consider issuing a another specific collection notice
Sensitive information about Employee	Employee or Third party	Consent implied if collect directly from employee. Seek employee's consent if collecting from third party.	Employees should be provided with an employee collection notice (which could be included with onboarding documents)
Sensitive information about Contractor / Third party	Contractor (information about Contractor) / Third party (information about third party)	Consent implied	Collection notice should be given unless obvious

Do's and Don'ts

DO only collect personal information that the School requires to carry out its functions and activities.

DO take reasonable steps (e.g. by providing a privacy collection notice) to ensure that, when collecting personal information, individuals are made aware of the following matters unless it is obvious or they would already know:

- the School's identity and contact details;
- if the individual may not be aware that the information has been collected, the fact that it has been collected and the circumstances of the collection;
- if collected under or authorised by law, the fact that the collection is so required or authorised (including details of the law requiring or authorising collection);
- why the information is being collected;
- the main consequences (if any) if the School does not collect all or part of the information;
- any other entities or types of entities to whom the information may be disclosed;
- that the School Privacy Policy contains information about how an individual can access and seek correction of information;
- that the School Privacy Policy sets out how an individual may complain about a breach of their privacy and how the complaint may be dealt with; and
- whether information is likely to be disclosed overseas and, if so, to which countries, if practicable to specify.

DON'T collect personal information from someone about another individual (e.g., next of kin details) unless it is unreasonable or impracticable for you to contact the individual directly.

DON'T collect (write down or otherwise record) unsolicited information if it is not reasonably necessary for a function or activity of the School. If unsolicited information is collected (e.g. it is received by email), delete or de-identify it if it is not reasonably necessary for a function or activity of the School.

Additional Do's and Don'ts for sensitive information

DO only use sensitive information for the purposes for which it was collected.

DO obtain consent if you collect sensitive information unless an exception applies or consent can be implied from the circumstances (e.g. an individual provides the individual's sensitive information directly to the School).

DON'T collect sensitive information unless it is necessary.

4. USE AND DISCLOSURE OF PERSONAL INFORMATION (APP 6)

4.1 Requirement:

A School must not use or disclose personal information about an individual other than in specified circumstances including:

(a) for the primary purpose for which it was collected (APP 6.1); or

(b) with the individual's consent (APP 6.1(a));

(c) for a secondary purpose which is related to the primary purpose of collection (or directly related in the case of sensitive information), and which the individual would reasonably expect (APP 6.2(a));

(d) where required or authorised by or under law (APP 6.2(b));

(e) where the School reasonably believes that the use or disclosure is necessary to lessen or prevent serious threats to the life, health or safety of any individual, or to public health or safety, and it is unreasonable or impracticable to obtain consent (APP 6.2(c));

(f) where the School has reason to suspect that unlawful activity, or misconduct of a serious nature, relating to its functions or activities has been (or may be) engaged in and the School reasonably believes the use or disclosure is necessary in order for it to take appropriate action (APP 6.2(c));

(g) where the School reasonably believes the use or disclosure is reasonably necessary to assist with locating a person reported as missing (APP 6.2(c)).

Primary and related purpose

4.2 Where the School collects personal information directly from the individual, the context in which the individual gives the information to the School will help identify the primary purpose of collection. When an individual provides, and the School collects, personal information, they almost always do so for a particular purpose – for example, to enrol a student or receive a service. This is the 'primary' purpose of collection, even if the entity has some additional purposes in mind.

4.3 How broadly a School can describe the primary purpose will need to be determined on a case-by-case basis and will depend on the circumstances.

4.4 Where a School collects personal information indirectly, a guide to its primary purpose of collection could be what the School does with the information soon after it first receives it.

4.5 Related and directly related purposes within reasonable expectations.

A School can also use and disclose the personal information for a related or, for sensitive information, directly related purpose where the individual has a reasonable expectation of that use or disclosure. To be related, the secondary purpose must be something that arises in the context of the primary purpose.

For sensitive information the use or disclosure must be directly related to the primary purpose of collection. This means that there must be a stronger connection between the use or disclosure and the primary purpose for collection.

4.6 Reasonable expectation

The test for what the individual would 'reasonably expect' would be applied from the point of view of what an individual with no special knowledge of the industry or activity involved would expect. The APP Guidelines provide that '*the 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP entity to be able to justify its conduct*'.

4.7 Factors to consider

When thinking about whether a use or disclosure falls within the primary purpose or a related or directly related purpose within the individual's reasonable expectations a School could, where relevant, consider:

(a) the context in which it is collecting the personal information;

(b) the reasonable expectations of the individual whose information it is;

(c) the form and content of information the School has given about why it is collecting the individual's information (for example under APP 1.4 and 5.2);

(d) how personal, confidential or sensitive the information is; and

(e) any duties of care or other professional obligations a School might have (although care would be needed if these are not within the person's reasonable expectations).

4.8 Secondary use and disclosure with consent (APP 6.1(a))

A School may use or disclose personal information for a secondary purpose if it has the individual's consent. Consent to the use or disclosure can be express or implied. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the School. If the School's use or disclosure has serious consequences for the individual, the School would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In such situations it would ordinarily be more appropriate for the School to seek express consent.

Use and disclosure of information about students – Table 4A

4.9 Personal information is used and disclosed by Schools about students for a variety of reasons. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies APP 6 on a case by case basis.

Use and disclosure of information about students – Table 4A

Category	Use & disclosure of personal and sensitive information about students
Primary purpose	*Personal information and sensitive information* • broadly to provide its educational services and exercise its duty of care (but the precise purpose will depend on the circumstances)
Secondary purpose (related)*	*Personal information* • send newsletters, magazines, mail-outs and correspondence • to include in newsletters, magazines and mail-outs (subject to comments in Section 3 of Part C of this Manual) • administration (e.g., records of attendance) • provide reports to parents
Secondary purpose (directly related)*	*Sensitive information* • compliance with law (e.g., immunisation records, Health Department) • assess eligibility and apply for funding and government grants • assess and address health issues and learning difficulties • provide medication and assistance when required (e.g., administering medication) • compiling health record lists and medication lists • doctor or hospital (for medical assistance) *In some cases these will be the primary purpose of collection

* Whether these uses and discloses are reasonably expected will depend on the circumstances, e.g. if the individual has been informed of the use or disclosure in a relevant collection notice or it is otherwise reasonably expected.

Use and disclosure of information about parents – Table 4B

4.10 Personal information about parents is used by Schools for a variety of purposes and disclosed by Schools to a variety of other parties. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies APP 6 on a case by case basis.

Use and disclosure of information about contractors – Table 4C

4.11 Personal information about contractors is used for a variety of purposes and disclosed by Schools to a variety of other parties. The following table illustrates some instances of such uses and disclosures. However, the School should consider whether a use or disclosure satisfies APP 6 on a case by case basis.

Use and disclosure of information about parents – Table 4B

Category	Use & disclosure of personal and sensitive information about parents
Primary purpose	*Personal information and sensitive information* • broadly to provide educational services to students and exercise its duty of care (the precise purpose will depend on the circumstances)
Secondary purpose (related)*	*Personal information* • send newsletters, magazines, mail-outs and correspondence • for meeting requirements of parents or court orders
Secondary purpose (directly related)	• Sensitive information compliance with law (e.g., a law relating to child protection - where a parent volunteers to drive a car for an excursion)
Direct Marketing	• fundraising • marketing for potential enrolments **See Section 5 of this Part D for a description of requirements applicable to the use and disclosure of personal information for direct marketing.**

Use and disclosure of information about contractors – Table 4C

Category	Use & Disclosure of personal and sensitive information about contractors
Primary purpose	*Personal information and sensitive information* • to engage the contractor
Secondary purpose (related)*	*Personal information* • to pay invoice (although this would be the primary purpose of collecting bank account information)
Secondary purpose (directly related)	*Sensitive information* • To manage workers' compensation claim (although this may be the primary purpose if the sensitive information is collected solely for the purpose of the workers' compensation claim)

* Whether these uses and discloses are reasonably expected will depend on the circumstances, e.g. if the individual has been informed of the use or disclosure in a relevant collection notice or it is otherwise reasonably expected.

How to comply

4.12 Before using or disclosing personal information on the basis that the use or disclosure is for a purpose that is related (or directly related in respect of sensitive information) to the primary purpose of collection, ensure the individual would reasonably expect the use or disclosure. For example, ensure the use or disclosure is listed in a collection notice that has been provided to the individual (or provide such a notice). See Section 3 of this Part D (in particular from Paragraph 3.25).

4.13 Schools need to consider their enrolment and employment forms through which personal information is collected to ensure that they include an appropriate collection notice (see from Paragraph 3.25 of this Part D).

Use or disclosure required by law (APP 6.2(b))

4.14 Comment

The Privacy Act does not override specific legal obligations relating to use or disclosure of personal information. 'Law' includes Commonwealth, State and Territory legislation, as well as common law. If an entity is required by law to use or disclose personal information it has no choice and it must do so. If an entity is authorised by law to use or disclose personal information it means the entity can decide whether to do so or not.

4.15 Disclosure authorised by law in New South Wales

In New South Wales, specific legislation authorises disclosure of personal information relating to a student, prospective student, staff volunteers and parents for certain child protection purposes.

How to comply

4.16 Where a disclosure is required as a result of a duty of care owed to an individual, then this may be done under APP 6.2(b) without the individual's consent. Similarly, where there is a legislative requirement to disclose information this may be done under APP 6.2(b) without the individual's consent.

4.17 Table 4D illustrates what steps should be taken by the School in deciding whether it can use or disclose personal and sensitive information.

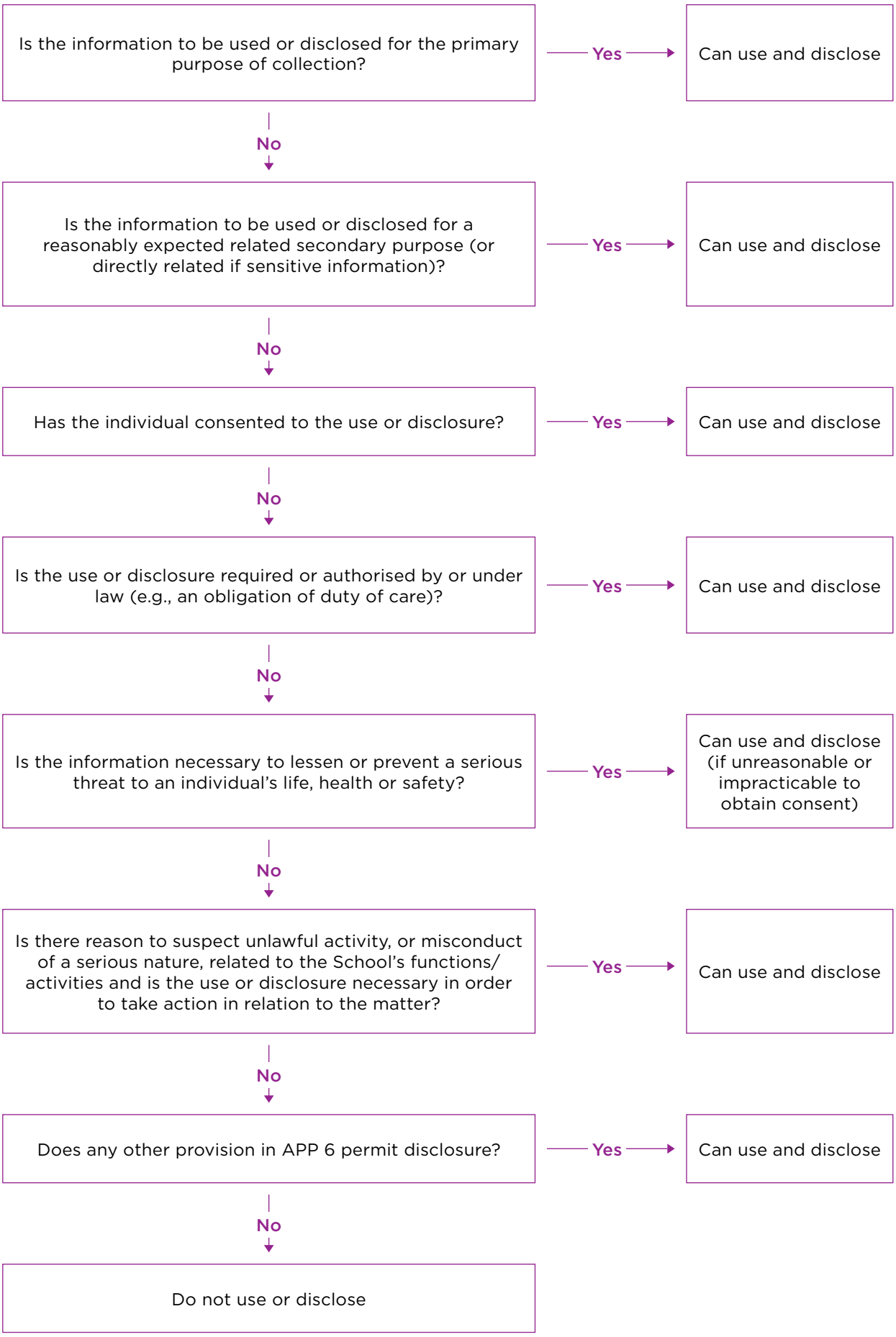
Do's and Don'ts

DON'T use or disclose personal information unless with consent, for the primary purpose of collection or for a reasonably expected related secondary purpose of collection (or *directly* related secondary purpose in the case of sensitive information) or where another exception applies, such as exercising duty of care.

DO make a written note of use or disclosure of personal information if used or disclosed under an exception in APP 6.2.

DO use or disclose an individual's personal information which is first collected by a related School only for the same primary purpose or reasonably expected related secondary purpose of collection of the related School.

Use and disclosure compliance steps – Table 4D



5. DIRECT MARKETING (APP 7)

Requirement:

A School must not use or disclose personal information it holds for the purpose of direct marketing, unless:

Scenario 1:

(a) it collects the information from the individual;

(b) the individual would reasonably expect the School to use or disclose the information for direct marketing; and

(c) there is a simple means by which the individual can request not to receive direct marketing, of which the individual has not availed him or herself (APP 7.2).

Scenario 2:

(d) either:

(i) it collects the information from the individual and the individual would not reasonably expect the School to use or disclose the information for direct marketing; or

(ii) the information is collected from a third party; and

(e) either:

(i) the individual has consented; or

(ii) it is impracticable to obtain consent; and

(f) there is a simple means by which the individual can request not to receive direct marketing; each direct marketing communication contains a prominent statement that the individual may request not to receive such communications; and the individual has not availed him or herself of this (APP 7.3).

Requirement:

If a School uses or discloses personal information for the purpose of direct marketing the relevant individual may request:

(a) not to receive direct marketing communications;

(b) that their personal information not be used by or disclosed to other entities for the purpose of facilitating direct marketing; and

(c) to be provided with the source of the information (unless it is impracticable or unreasonable to do so).

Requirement:

Sensitive information may not be used or disclosed for the purpose of direct marketing unless the individual has consented (APP 7.4).

Requirement:

Instruments such as the *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth) will displace the requirements of APP 7 (APP 7.8) (to the extent that instruments apply to the School).

Comment

5.2 The APP Guidelines provide that 'direct marketing' involves the use and/or disclosure of personal information by a School to communicate directly with a person to promote goods and services. The direct marketing communication could be delivered by a range of methods including mail, telephone, email, app or SMS. A campaign to boost enrolments is an example of a direct marketing campaign by a School.

5.3 Direct marketing is addressed separately within a discrete principle rather than as a kind of secondary purpose (see APP 6) because of the significant community interest about the use and disclosure of personal information for the purposes of direct marketing.

5.4 The principle distinguishes between individuals, such as existing or previous customers, who have been in contact with an entity, and those who have not. The intention is to apply more stringent obligations when using personal information of individuals who have no pre-existing relationship with an entity, as those individuals would be less likely to expect their information to be used or disclosed for direct marketing purposes.

5.5 A School may use non-sensitive personal information for direct marketing where, among other things, the School collected the information directly from the individual, the individual would reasonably expect their information to be used or disclosed for direct marketing, and there is a simple means by which the individual can request not to receive

direct marketing material. A School may not use sensitive information for direct marketing unless it has obtained consent to do so.

5.6 *'Reasonable expectation'*

Considering whether an individual has a 'reasonable expectation' that their personal information may be used for direct marketing involves balancing a number of factors that could include:

(a) the content of any collection notice/s provided to the individual, as well as the School's privacy policy;

(b) the way a School communicates with an individual;

(c) the previous types of communications between a School and an individual;

(d) how often the School is in contact with an individual; and

(e) the duration of a School's relationship with an individual

The question of 'reasonableness' would generally be considered at the time of the proposed use of the personal information for direct marketing – not the time the personal information was collected.

How to comply

5.7 If a School wishes to use or disclose personal information for direct marketing, the School should first consider whether:

(a) the personal information was collected from the individual; and

(b) the individual would reasonably expect the School to use or disclose the information for direct marketing.

5.8 If the answer to either of those questions is no, then the School will need to rely on APP 7.3 to use or disclose the personal information for direct marketing. If so, the individual's consent must be obtained or it must be impracticable to obtain their consent.

5.9 The APP Guidelines state that in considering whether it is 'impracticable' to obtain consent will depend on a number of factors, including the time and cost involved in seeking consent. However, an organisation is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

5.10 The APP Guidelines provide that an organisation may obtain the consent from the individual in relation to a subsequent use or disclosure of the individual's personal information for the purpose of direct marketing at the time it collects the personal information. In order to rely on this consent, the organisation must be satisfied that it is still current at the time of the use or disclosure.

5.11 Where an organisation did not obtain the individual's consent at the time of collection, it must obtain the consent of the individual for the proposed use or disclosure, unless it is impracticable to do so (or unless APP 7.2 applies). In that case, the organisation should assess whether it is impracticable to obtain consent at the time of the proposed use or disclosure.

5.12 Each direct marketing communication should include a simple means by which the individual may request not to receive direct marketing communications, and a prominent 'opt-out' statement which should be brought to the individual's attention. An example for direct marketing sent by post would be:

> Direct marketing opt-out
>
> If you do not wish to receive any further fundraising/direct marketing communications from us, please tick the box below and return this [form] to [us].
>
> ☐ No, I do not wish to receive fundraising/direct marketing communications.

6. CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION (APP 8)

6.1 Requirement:

If a School discloses the personal information of an individual to a person outside Australia (other than internally or to the individual themselves) it must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1). It may however be held liable for any acts done or practices engaged in by the overseas recipient which are found to be a breach of the APPs. A School will not be required to comply with this provision in some limited circumstances, including where:

(a) the School reasonably believes that the overseas recipient is bound by privacy laws which are substantially similar to the APPs **AND** there are mechanisms which the individual can take to enforce those laws (the '**Reasonable Belief Defence**'); or

(b) the individual consents to the disclosure having been expressly informed that the overseas recipient may not be required to provide the same protections as are provided by the APPs and, if there is a breach by the recipient, the School will not be accountable and the individual will not be able to seek redress under the Privacy Act; or

(c) the disclosure is required or authorised by law.

How to comply

6.2 APP 8 regulates the cross-border disclosure of personal information outside of Australia. Unless an exception applies, it requires Schools to take 'reasonable steps' to ensure the overseas recipient handles the personal information the School discloses to it in a way that does not breach APPs 2-13.

6.3 If a School relies on having taken 'reasonable steps' or an exception does not apply, and the overseas recipient handles the information received from the School in breach of the APPs, the School may be liable for the breach.

6.4 The provisions of APP 8 will be triggered where a School chooses to disclose personal information to an overseas recipient. For example, this could occur where a School in Australia:

(a) liaises with a School located overseas to facilitate a student exchange;

(b) liaises with overseas companies to arrange an overseas school trip;

(c) outsources data storage and handling functions to a third party 'cloud' service provider whose servers or personnel are located overseas (however, there are circumstances in which this will not be a 'disclosure' – this is explained below); or

(d) uses online or 'cloud' service providers to provide services to the School that involve personal information, such as services relating to email, instant messaging and education Apps, whose servers or personnel are located overseas (however, there are circumstances in which this will not be a 'disclosure' – this is explained below).

6.5 Online or 'cloud' service providers (referred to in Paragraphs (c) and (d) above) use servers (as well as personnel) that may be located outside Australia, sometimes in multiple or changing locations. If the server (and/or personnel) is located outside Australia, it is important the school can get assurances that the personal information will be handled and protected in accordance with the APPs. It is also important that Schools are aware of the practices of the cloud provider and enter into appropriate arrangements to limit their exposure should a data breach occur. The use of a cloud service provider by a School *may* trigger the requirements under APP 8. However, the APP Guidelines provide that where a School provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the School may access the personal information, the provision of the information may be a '*use*' and not a '*disclosure*' (and therefore APP 8 will not apply) where:

(a) the contract between the School and the overseas cloud service provider binds the provider only to handle the personal information for the limited purpose of performing

the services of storing and ensuring the School may access the personal information;

(b) the contract requires any sub-contractors to agree to the same obligations; and

(c) the contract between the School and the cloud service provider gives the School effective control of how the personal information is handled by the cloud service provider.

6.6 As this interpretation in the APP Guidelines has been questioned by some, there is still a reference to using an offshore cloud service for storage in the template collection notices and privacy policies Annexed to this Manual. Schools should make their own assessment of whether their use of online or 'cloud' service providers (or other offshore providers) is a '*use*' or '*disclosure*' of personal information and update their collection notices and privacy policy accordingly.

6.7 If a School is using an offshore cloud service in circumstances where this is a '*disclosure*' of personal information, the School will also be required to advise people in collection notices and its privacy policy that their personal information may be disclosed or sent offshore and, if known, to which countries.

6.8 In circumstances where personal information is likely to be disclosed overseas, the School disclosing the information must have procedures in place for ensuring that requirements contained in APP 8.1 are complied with or establishing that it can rely on an exemption in APP 8.2.

6.9 Although it will depend on the circumstances, generally compliance with APP 8 can be achieved if the overseas recipient is in a country that has been prescribed in regulations made under the Privacy Act or the School:

(a) enters into a contract with each intended overseas recipient of the information which requires that recipient (and any subcontractors) to agree that the information will be dealt with in a manner that complies with the APPs (NB schools will remain liable for breaches of the APPs by overseas recipients). Depending on the nature of the personal information, the School may also need to conduct due diligence on the overseas recipient before disclosing the personal information; or

(b) reasonably believes that the recipient of the information is subject to a law or a binding scheme which provides similar protection to the APPs and which the individual can enforce. This would be achieved, for example, where personal information is disclosed to an organisation situated in a member country of the EU as they have privacy laws offering similar protection to those contained in the APPs (NB no local liability for any breaches); or

(c) obtains a consent from the individual to the disclosure, after being told that the protections provided under the APPs may not apply and the School will not be accountable and there will be no redress under the Privacy Act. If Schools wish to rely upon this exception they should seek specific advice on the form of notice and the nature of the consent will have to be specifically drafted to meet the particular situation (NB no local liability for any breaches and consent may be withdrawn at any time).

6.10 It is strongly suggested that if a School enters into a contract with a recipient of personal information, as well as seeking undertakings to protect the information they should seek also an indemnity from the recipient to protect the School against claims in the event of a data breach.

6.11 Schools that use applications or services through which personal information is processed, such as Google Apps for Education or Office 365 need to be aware that through the use of these services, personal information of students, parents or guardians may be transferred, stored and processed by the service providers overseas. If a School uses such applications or services it should conduct due diligence, including in particular on security. As part of this due diligence, the School should review the provider's privacy policy and terms and conditions of use to confirm appropriate handling and security of the personal information, or enter into a contract with the provider that should:

(a) require the provider to ensure the School has continued access to any

personal information on its system and ongoing system support anytime/anywhere;

(b) require the provider to deliver a secure user account and login facility;

(c) require the provider to handle all personal information in accordance with relevant privacy laws;

(d) require the provider to only use and disclose the personal information for the purpose of providing the services only or otherwise only as authorised by the School;

(e) place stringent conditions on the provider to maintain security of the data, accept responsibility for any breach and assist the School in the event of a breach or a complaint or investigation (and indemnify the School in the event of a breach);

(f) entitle the School to audit the system and information; and

(g) allow the School to withdraw the information at any time and requires return or destruction of the data on the expiry or termination of the service.

6.12 If a School needs to disclose personal information for a particular purpose in specific circumstances (e.g., a particular overseas excursion or school exchange) it could seek a consent prior to the disclosure for that particular purpose. An example would be:

Consent to overseas disclosures

I/We consent to the disclosure of our personal information/the personal information of [***name***] to [***identify overseas recipient or class of recipients***] for the purpose of [***e.g., facilitating a student exchange***].

* I/We acknowledge that we are aware that [***identify overseas recipient or class of recipients***] may not be bound by laws which provide the same level of protection for personal information provided by the Australian Privacy Principles and that, if [***identify overseas recipient or class of recipients***] handles the personal information in breach of the Australian Privacy Principles, the School will not be accountable under the Privacy Act and I/we will not be able to seek redress under the Privacy Act.

*If applicable

6.13 A number of students attending various Schools are full fee paying overseas students (i.e., the students' parents are located overseas). It can be reasonably assumed that the sending of personal information about the student to the parents will not cause an issue. If however the parents or student require personal information to be sent to a third party overseas an express consent should be obtained.

Do's

DO take care when disclosing information overseas.

DO investigate the privacy obligations of overseas recipients of personal information, rather than simply taking their word for it, if you intend to rely upon the Reasonable Belief Defence. Do this by reviewing their privacy policy and terms and conditions of service/use.

DO ensure that 'cloud' providers and other overseas service providers provide appropriate undertakings, warranties and indemnities.

DO advise people if their information will or may be sent offshore and if practicable where it will be sent.

DO obtain consents for one-off transfers of information where it is practicable to do so.


www.

7. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS (APP 9)

7.1 Requirement:

APP 9 requires that identifiers assigned by a government agency, such as a Medicare number or a drivers licence number cannot be:

(a) adopted by a School as its own identifier to identify an individual unless required or authorised by law; and

(b) used or disclosed unless it is reasonably necessary to verify the identity of the individual or to fulfil its obligations to an agency or State or Territory authority, or is required or authorised by law (there are also other specific exceptions).

Comment

7.2 A government related identifier (**GRI**) is a unique combination of letters, numbers and/or symbols which Commonwealth agencies or State or Territory authorities (or their agents or contracted service providers) allot to an individual. Examples include a Medicare number, a driving licence number, a passport number, a Centrelink reference number, student identification or registration numbers issued by a Department of Education, ACARA or other State or Commonwealth authority (**Student Identifier**) or a platform student identifier (**PSI**) created for NAPLAN online.

7.3 APP 9 seeks to ensure that increasing use of GRIs does not lead to a de facto system of universal identity numbers, and to prevent any loss of privacy from data-matching facilitated by the use and disclosure of GRI.

7.4 For these reasons, specific tax file number (**TFN**) legislation already restricts the way an organisation can collect, use or disclose a TFN.

7.5 APP 9 restricts the adoption, use or disclosure of GRIs, unless an exception applies. An individual cannot consent to the adoption, use or disclosure of their GRI, it must fall within one of the exceptions. APP 9 does not prohibit the collection of GRIs (although the collection will be regulated by APPs 3 or 4, and 5, in respect of which see Section 3 of this Part D of this Manual).

7.6 APP 9 does not apply to an individual's name.

How to comply

7.7 The School must ensure that it does not adopt as its own identifier a GRI, unless the adoption is required or authorised by Australian law or court/tribunal order or is permitted by regulations made under the Privacy Act. A school 'adopts' a GRI as its own identifier of an individual if the school organises the information that it holds about that individual with reference to that GRI. That is, it uses the GRI as the means to identify the individual within its files or systems. The School should ensure that staff are not able to enter a person's GRI (such as a Medicare number or Student Identifier) into a database in order to retrieve their record.

7.8 Additionally, when using or disclosing GRIs, the School must ensure that such use or disclosure is permitted by APP 9 (e.g., where the use or disclosure is reasonably necessary to verify the identity of the individual or for the School to fulfil its obligations to a Commonwealth agency or a State or Territory authority, or the use or disclosure is required or authorised by law).

7.9 In relation to the platform student identifier created for NAPLAN online, the National Schools Interoperability Program (in consultation with other stakeholders) has developed guidelines to assist stakeholders (such as Schools) in their usage of the NAPLAN online PSI. Schools should consult these guidelines before using and/or disclosing such identifiers.

Do's and Don'ts

DO only use identifiers which are created by the School to identify individuals, not GRIs.

DON'T create databases that allow an individual's GRI to be entered in order to retrieve a record about the individual.

DON'T leverage off GRIs as a means of tracking students throughout their schooling life.

DON'T use or disclose GRIs unless it is necessary to fulfil an obligation to a government agency or authority, it is required or authorised by law, or it is necessary to verify a person's identity. An individual's TFN should never be used as an identifier.

8. DATA QUALITY (APP 10)

8.1 Requirement:

A School must take reasonable steps to ensure that personal information it:

(a) collects is accurate, complete and up-to-date; and

(b) uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

8.2 A School should establish procedures for updating records, passing on changes, deleting records that are no longer used or required and contacting entities to which the records have been disclosed (to inform them of changes).

Comment

8.3 The aim of APP 10 is to prevent adverse consequences for people that might result from a School collecting, using or disclosing inaccurate, incomplete or out-of-date personal information.

8.4 APP 10 requires that information used or disclosed must be relevant to the purpose for which it is to be used or disclosed. If the purpose of disclosure is not clear this may require a School to inquire about the purpose before making the disclosure.

8.5 Reasonable steps to confirm the accuracy, completeness and currency of the personal information a School collects only need to be taken at the time it collects, uses or discloses the information (unless there are circumstances indicating that the information is incorrect, in which case the School must comply with APP 13 – see Section 11 of this Part D). It is important that information is checked at times it is to be used or disclosed to determine if it is not accurate, complete, up-to-date or relevant.

How to comply

8.6 The School should establish standard procedures to ensure that the personal information it collects, uses or discloses is accurate, complete, up-to-date and relevant.

8.7 The reasonableness of the measures taken would depend on:

(a) whether the information is the type that would change over time;

(b) how recently the information was collected;

(c) the reliability of the information; and

(d) who provided the information.

8.8 The School is not necessarily required to check and re-check all records of personal information for accuracy, completeness, relevancy and currency in all circumstances, but only when it is to be used or disclosed.

8.9 In order to achieve compliance, procedures should be adopted to ensure that:

(a) records containing sensitive information such as health information be checked for accuracy before being used or relied upon;

(b) there is a regular audit of all records of personal information held, whereby records that are not used or required are disposed of and inaccurate records updated;

(c) if records are to be disclosed, there is a check on relevance of the records disclosed and their accuracy;

(d) records are de-identified or destroyed when no longer needed by the School; and

(e) either in conjunction with the 'regular audit' or otherwise, a periodic 'mail-out' is made to the information provider, providing an opportunity to update, and ensure the accuracy of, their personal information.

Sharing personal information

8.10 Where personal information is shared between 'related Schools' or between Schools in the same system, the disclosing and receiving School should keep records as to whom the personal information was disclosed or/collected from. Once either School becomes aware of any change in the personal information then that School may then pass on such changes and corrections to the other School. This will help ensure that the information held by both Schools is consistent and remains accurate and up-to-date. See Paragraph 15.4 of Part C regarding the related companies exemption.

8.11 What procedures are put in place in this regard will likely depend upon the size of the School.

Do's and Don'ts

DO be familiar with the School's systems to ensure accurate and up-to-date personal information is kept.

DO consider the age of personal information, and whether the information is likely to change (e.g., an address is more likely to change rather than a name), in determining whether it is likely that the information is inaccurate, incomplete or out-of-date.

DO, when passing personal information internally or to a related School, notify the other party of the age of the information if this is likely to affect its accuracy and currency.

DO consider the impact if the information is incomplete, inaccurate or out-of-date (e.g., health information) and take appropriate steps.

DO investigate any clear inconsistencies with personal information held (e.g., recorded as a male, but is an ex-student in an all girl school).

DO consider whether the information was collected directly from the individual and whether it is a reliable source.

DO give the individual a chance to comment on the information provided, if reasonable and practicable to do so.

DO, where practicable, check personal information with existing records collected for the same or a related purpose to see whether it is consistent, accurate and up-to-date before using or disclosing personal information.

DO try to provide individuals with user friendly ways to update their information.

DO keep records accurate by notifying a related School from/to which personal information is collected/disclosed of any changes to the information, and keep a record for such notification.

DO check with a person to whom information is to be disclosed about the disclosure, if this is not clear.

DON'T continue to use information you believe to be out of date or inaccurate.

9. DATA SECURITY (APP 11)

9.1 Requirement:

A School must take reasonable steps to protect personal information it holds from misuse, interference and loss, and unauthorised access, modification or disclosure.

The APP's now explicitly provide that such steps include technical and organisational measures.

9.2 As previously noted, Schools collect large amounts of personal information ranging from names and addresses to health information, identity documents and credit card details. The unauthorised disclosure of or access to this information can have serious consequences, both personal and financial. Increasingly sophisticated methods of storing and accessing stored information have paradoxically also provided greater opportunities for misuse.

9.3 The level of security should be in proportion to the risk to the individual if their personal information is not secured. Therefore extra care must be taken to ensure that very confidential information is particularly secure. People generally expect that their identity documents (e.g. birth certificate), financial information and sensitive information (particularly health information) will be afforded a high level of protection.

9.4 The requirement that reasonable steps must be taken to prevent 'interference' with personal information is intended to cover the unlawful accessing of electronic databases.

9.5 A difficulty for Schools is that they usually do not have single entry points for data or one consistent system of storage and access. In dealing with security this is a factor that needs to be taken into account.

9.6 The OAIC has published a Guide to securing personal information (**the Security Guide**), which can be accessed at:

https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information.

It is recommended that those responsible for compliance with APP 11at the School consider the Security Guide.

Typical areas of concern

9.7 Five typical areas of concern are set out below:

(a) Physical security

- Is personal information contained in hard copy form kept in locked filing cabinets in lockable rooms?
- Are there alarm and security systems in place?
- Is personal information held in electronic form held in a secure location with limited access based on a need-to-know basis?
- Is the storage and movement of files audited and monitored?

(b) Logical security

- Are the latest technology firewalls, data encryption and anti-intrusion devices installed and running?
- Are ICT systems and processes tested regularly?

(c) Access and use management (both physical and logical)

- Are there policies in place to restrict access which are administered by a dedicated staff member?
- Are access and use restrictions audited?
- Are staff trained in the privacy policies and procedures?

(d) Storage protocols

- Is there a classification for how documents should be stored, both onsite and offsite?
- Are there procedures in place for removal of documents which are no longer to be retained?

(e) Internet and/or 'cloud' services providers

- Have they demonstrated a robust security system and provided the School with appropriate undertakings, warranties and indemnities to protect and be responsible for the safe keeping of the data?
- Are they located offshore and if so where?


PERSONAL INFORMATION
FIRST NAME
ADDRESS
CITY
PHONE
PART 1
PHONE

Reasonable steps

What are 'reasonable steps' to secure personal information will depend on the School's particular circumstances. The Security Guide indicates that some relevant factors could include:

(f) the nature of the entity holding the personal information;

(g) the amount and sensitivity of personal information held;

(h) the possible adverse consequences for an individual in the case of a breach;

(i) the practical implications of implementing the security measure, including time and cost involved; and

(j) whether a security measure is in itself privacy invasive,

How to comply

9.8 The School should ensure hard copy records containing more confidential information are secured in locked cabinets with restricted access and building alarms or similar security measures.

9.9 Where there is a potential for unauthorised access to personal information, for example, health information (or any other personal and sensitive information) is displayed or distributed to staff members, steps should be taken to ensure that the potential for unauthorised access to that information is minimised.

9.10 If some personal information about students is on display in the staff room it is important to consider whether it is necessary for it to have such wide distribution. If it is, care should be taken to restrict outside access to the staff room.

Example:

If some children's names and their medication requirements were openly displayed in a classroom, then this would be likely to breach APP 11.1. However, if such information was only kept in a locked safe which would be difficult to access in the event of an emergency, then this would exceed what is required under APP 11.1 (and may put the child's health at risk). A common sense approach should prevail so that the information was readily available but not publically displayed.

9.11 Staff members taking records of personal information outside School grounds (e.g., school assignments and laptop computers) should be reminded about the need to keep personal information secure, especially in the case of sensitive information where the adverse consequences of unauthorised access may be high.

9.12 The School should develop and enforce a policy on remote access to School systems. Steps should be taken to ensure the remote access is secure.

9.13 If electronic records of personal information are kept, steps must be taken to ensure that personal information contained in databases is appropriately secure. This would often include having restricted access, passwords that limit such access and other appropriate measures to prevent unauthorised access to records. Additionally, the School must continue to ensure that appropriate firewalls and other security technology is applied to protect electronic records of personal information. This will also apply to the security of electronic communications that contain personal information.

9.14 Extra protection should be given to copies of identity documents (birth certificates, passports, driver's licences) given the risk of identity fraud if these documents are stolen. Hard copies should be stored in locked cupboards and electronic copies securely encrypted. Both hard and electronic copies should be accessible by staff purely on a need to know basis, and should be securely deleted as soon as they are no longer needed by the School. The School should consider whether it needs to retain a copy of identity documents, or if it can retain a subset of the information within the document instead.

9.15 The need for policies and security measures in respect of computer, email and Internet use should be reviewed.

9.16 Appropriate warnings to staff to ensure that passwords are not divulged and that electronic records are not accessed by unauthorised means should be contained in computer or Internet use polices. A number of data breaches have occurred where staff have provided their passwords to students.

9.17 The School should have in place comprehensive confidentiality and security procedures and provide training to all individuals who have access to personal information (such as employees and contractors) as to the appropriate manner in which personal information should be treated.

9.18 These procedures should be regularly monitored and audited for compliance to ensure their effectiveness. If a data breach occurs, immediate steps should be taken to prevent a repetition of the circumstances giving rise to the breach.

Use of the Internet and emails

9.19 For collection of personal information through websites (where relevant), the School must ensure that the data is stored securely to prevent unauthorised access. Reasonable steps will need to be taken to ensure that any information provided over the Internet, for example through online enrolments, is secure.

9.20 Reasonable steps must be taken so that email communications, and the personal information contained therein, are secure in order to prevent unauthorised access.

Destruction and permanent de-identification (APP 11.2)

9.21 Requirement:

Where personal information is no longer required for an authorised purpose, a School must take reasonable steps to destroy or permanently de-identify the personal information.

Comment

9.22 A School should have in place systems for destroying or de-identifying personal information that is no longer needed.

9.23 Destruction of records containing personal information should be by secure means. Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction and should only be used for documents that are already in the public domain. Reasonable steps to destroy paper documents that contain personal information include shredding, pulping or disintegration of paper. For particularly sensitive information or information that may put the individual at risk, the shredded etc paper should be securely disposed of (not simply thrown in the bin).

9.24 The reasonableness of steps taken to destroy personal information contained in electronic records will depend on the medium within which the data is stored and the available methods for erasing data.

9.25 The APP Guidelines provide that where it is not possible to irretrievably destroy personal information held in an electronic format, reasonable steps to destroy it would include putting the personal information 'beyond use'. This means that the organisation is unable, and will not attempt, to use or disclose the personal information; cannot give any other entity access to it; surrounds it with appropriate technical, physical and organisational security (including, at a minimum, access controls including logs and audit trails); and commits to take reasonable steps to irretrievably destroy it if, or when, this becomes possible. As an alternative to putting information 'beyond use', a school could instead take reasonable steps to de-identify the personal information.

9.26 The APP Guidelines provide that it is expected that only in very limited circumstances would it not be possible to destroy personal information held in electronic format. An example of such limited circumstances is where it is impossible to destroy the personal information without also destroying other information which the school is required to retain.

9.27 Schools may also refer to the Australian Society of Archivists' Records Retention Schedule for Non Government Schools available at http://www.archivists.org.au/products/digital-downloads/records-retention-schedule-for- non-government-schools.

However, it should be noted that 'permanent archiving' of material does not constitute 'destruction'.

How to comply

9.28 Personal information which is no longer required for an authorised purpose should be destroyed or permanently de-identified.

9.29 In determining whether information is no longer required under APP 11.2 the School should have regard to a number of matters, including:

(a) whether there is a legal requirement to retain the information;

(b) whether it is likely that the information will be required at a later date for a purpose permitted under the APPs; and

(c) whether destroying the information would likely have a prejudicial effect on the School's operations.

9.30 It is common practice for records to be retained for at least 50 years in child protection matters.

9.31 Schools may also wish to discuss with their insurer and/or legal adviser what records should be kept and for how long.

9.32 When personal information is 'no longer required' will be a matter for the School to determine. As long as a policy to retain data can be reasonably justified there will be no infringement of this APP. This is a risk assessment issue for the School.

If there is a conversion of information collected from hard-copy records to electronic databases, it is important to consider whether it is possible and appropriate to destroy or permanently de-identify the information in the hard-copy record as soon as practicable after it is processed into the electronic form. In some cases this may be inappropriate.

Example:

Some Schools consider it appropriate to update incorrect information on a database but retain the original (and now inaccurate) information in the original form in which the information was initially collected. The keeping of original records in such circumstances may be appropriate where the original record is required to compare a change in an individual's medical condition, learning development or progress, or where it is necessary to retain the original record to verify what information was originally provided. However, in other cases it may be more appropriate to discard information contained in a hard-copy form which has been converted to electronic form, for example, a leave request form. However, this will depend on the situation and type of information contained in the form.

9.33 In cases where it is considered necessary to retain information that is old or superseded, steps must be taken to ensure that this old or inaccurate information is not confused with the new up-to-date accurate information. This is especially so where the information concerned is sensitive information and the consequence of relying on the old or incorrect information is adverse or detrimental to, or embarrassing for, the individual.

9.34 Further, in the case of both electronic or hard-copy records, the School must ensure that procedures are in place whereby records that are no longer required are de-identified or destroyed. The destruction of information must be done by secure means (e.g., securely locked bins, shredding, pulping) and not by general disposal. A fixed annual review of personal information would be a way to ensure that this obligation is complied with.

Do's and Don'ts

DO consider how, and in what form, you store personal information, and consider how secure this is.

DO ensure that all hard-copy records of personal information are kept securely locked or supervised.

DO ensure copies of identity documents (such as birth certificates, driver's licences and passports) are encrypted when stored and deleted as soon as the School no longer needs them.

DO locate personal information that is no longer needed. In such cases, the information should be destroyed or de-identified.

DO ensure that staff maintain adequate security of all personal information under their control.

DO limit access to personal information only to those who require it to carry out their duties for a permitted purpose (i.e. a 'need to know' basis).

DO contact the School's privacy officer if you are unsure as to the company's practices and procedures for keeping personal information secure.

DO make a note of to whom personal information has been disclosed, for example, a record of who has a particular file, or who has access to a particular database.

DO scrutinise requests for disclosure of personal information, for example follow the School's procedure to identify an individual who asks you to disclose or 'check' their personal information.

DO ensure that in case of shared computers, tools are implemented to avoid possible privacy breaches.

DO ensure that staff log in and out in accordance with allocated level of access.

DO establish procedures for the destruction or de-identification of personal information which is no longer required.

DO consider the following matters when engaging a cloud service provider:

- the sensitivity of the data from a privacy perspective;
- the sensitivity of the data from a business operational perspective;
- in what jurisdictions may the data be stored by the cloud provider;
- is the data encrypted when transferred and stored; and
- what other forms of security does the provider use.

DO ensure the cloud service provider is subject to strict contractual provisions regarding security of the data and liability for any breach.

DON'T access, discuss, display, or disclose personal information other than as permitted by the APPs.

DON'T leave personal information unattended and not secure. For example, if staff leave their computers they should password lock their screen (or turn off the computer if leaving for an extended period of time). Don't leave files where they may be accessed by unauthorised people.

DON'T ever allow unauthorised access, modification or disclosure of personal information.


Username
Password
Remember me
Forgot password
Login

10. ACCESS (APP 12)

10.1 A School must on request provide the individual with access to his or her own personal information that it holds about them.

10.2 However, there are some exceptions, including where:

(a) the School reasonably believes that providing access would pose a serious threat to the life, health or safety of any individual, or to public health or safety (APP 12.3(a));

(b) this would unreasonably impact on the privacy of other individuals (APP 12.3(b));

(c) the request is frivolous or vexatious (APP 12.3(c));

(d) the information relates to existing or anticipated legal proceedings between the parties, and the information would not be accessible through discovery (APP 12.3(d));

(e) access would reveal the intentions of the School in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e));

(f) this would be unlawful (APP 12.3(f));

(g) denying access is required or authorised by or under law (APP 12.3(g));

(h) the School has reason to suspect that unlawful activity or misconduct of a serious nature that relates to its functions or activities has been engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter (APP 12.3(h));

(i) providing access is likely to prejudice enforcement related activities conducted by or on behalf of an enforcement body (APP 12.3(i)); and

(j) providing access is likely to reveal evaluative information generated within the School in connection with commercially sensitive decision-making processes (12.3(j)).

10.3 The School must respond to the request within a reasonable period after the request is made, and give access to the information in the manner requested by the individual where it is reasonable and practicable to do so (APP 12.4).

10.4 Where access is denied in the manner requested by the individual, the School must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the School and the individual (APP 12.5).

10.5 Where access is denied, the School may consider whether the use of mutually agreed intermediaries would allow sufficient access (APP 12.6).

10.6 The School must not charge excessive fees for providing access, and must not charge for the making of the access request (APP 12.8).

10.7 Where access is denied, the School must give written notice of the reasons for refusal (except where unreasonable to set that out) and the mechanisms available to complain about the refusal (APP 12.9).

Comment

10.8 Detailed comment on common issues that arise in Schools in the context of APP 12 is at Section 5 of Part C of this Manual.

Unreasonable impact on the privacy of others

10.9 Access to a document containing personal information about people other than the individual requesting access need not be denied altogether. For example, in such a case, it may be possible to delete the other individual's personal information from the document before it is released to the individual who made the request.

10.10 Information that could have an unreasonable impact on another person's privacy can include more than information such as name and address. It could include any information about a reasonably identifiable individual.

Example:

Student A's parents ask for records from a School in relation to an investigation of a fight between students where a student was injured. The records disclose the name of various students who have given statements implicating Student A as having started the fight and causing the injuries. Providing access to records which identified the students who provided those statements would be likely to have an unreasonable impact upon them.

Frivolous or vexatious requests

10.11 Frivolous and vexatious requests could include those that are:

(a) requests that contains offensive or abusive language, or that do not appear to be a genuine request for personal information;

(b) repeated requests for access to the same personal information (which the School has already provided or has earlier explained that it does not hold); and

(c) requests made for the apparent purpose of harassing or intimidating the School's staff, or interfering unreasonably with its operations.

Access would be unlawful or denial of access is required or authorised by law

10.12 Providing access to personal information would be considered to be unlawful where it would constitute a breach of confidence under the law. Denial of access may be required or authorised by a State, Territory or Commonwealth law, or the common law (including a duty of care). Common law duties are discussed in Section 8 of Part C. If a School is required by a law to refuse access it must refuse access. If a School is authorised by law to refuse access it means it may decide whether to provide or refuse access.

How to comply

10.13 The School should establish a standard procedure whereby individuals are permitted to access their records except where an exception to the access principle applies. The School is entitled to make a charge for providing access on a cost recovery basis, but must not charge the individual to make the request for access.

10.14 Prior to collecting any personal information, the School should ensure that it has systems in place to respond to access requests within a reasonable period of time and determine whether access should be granted. Access requests could be made through the School's privacy officer or the Principal. The School should also implement practices, systems and procedures to enable the School to deal with inquiries and complaints about its compliance with the access provisions.

10.15 Although individuals are not required to give a reason to access their records, Schools should ask the individual what information or the type of information he or she wants access to. This is likely to help facilitate the individual accessing the information he or she is seeking.

10.16 APP 12 only gives individuals the right to access personal information which the School holds about that individual in a record the School possesses or controls. School staff should be made aware that any personal information a School holds can be the subject of an access request. This includes file notes and emails. However, this should not dissuade staff from making appropriate file notes of, or communicating, incidents.

10.17 A School should take adequate steps to verify the identity of the individual requesting access. This may include verifying that an individual has been given authority to access personal information on behalf of another individual. Such steps are likely to vary on a case by case basis. However the School should adopt the view that, in most cases, parents may have access to records relating to their child unless special circumstances arise. This is considered further in Section 5 of Part C of this Manual.

10.18 A School may refuse or restrict access to the record where an exception applies (such as where providing access would have an unreasonable impact on the privacy of others (APP 12.3(b)) or where the School has reason to suspect that unlawful activity or misconduct that relates to the School's functions or activities has been engaged in and providing access would prejudice the taking of appropriate action by the School (APP 12.3(h)).

Example:

An example of being permitted to refuse access is where a 'Report by Student Form' in relation to an incident is not to be made available to 'other' students. This could possibly include students who are the subject of the incident and report (e.g., in the case of bullying).

10.19 APP 12 requires that organisations must provide written reasons for denial of access and the mechanisms available to complain about the refusal. The reasons may be framed so as not to defeat the purpose of denying access (e.g., so as not to highlight to a 'suspect' requesting access that an investigation into their activities or misconduct is underway and providing access to their personal information would prejudice the investigations). It is prudent to retain a copy of those written reasons in order to avoid any confusion in the event of a dispute.

Giving access by other means

10.20 Where a School refuses to give access on a permitted ground, or refuses to give access in the manner requested by the individual, the School must take reasonable steps to give access in a way that meets the needs of the School and the individual. This is intended to ensure that entities work with individuals to try to satisfy their request.

10.21 The APP Guidelines provide that the following may be alternative manners of access that may meet the needs of the School and the individual:

(a) deleting any personal information for which there is a ground for refusing access and giving the redacted version to the individual;

(b) giving a summary of the requested personal information to the individual;

(c) giving access to the requested personal information in an alternative format;

(d) facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes;

(e) facilitating access to the requested personal information through a mutually agreed intermediary.

Example:

An example of using an intermediary is where access is requested to a student's file which includes personal information of other students which cannot be disguised. Rather than providing the entire file, it may be that a discussion with a teacher sufficiently satisfies the request for information.

Time periods

10.22 A School must respond to access requests within a reasonable period after the request is made. It is intended that a 'reasonable period' will not usually exceed 30 days.

Particular issues

10.23 Various issues might arise where a student seeks access to their personal information contained in records held by the School. Where a record of personal information about a student contains information which would normally not be released, the School would need to consider whether it may refuse or restrict access under APP 12.

10.24 Examples of scenarios where a School might consider restricting access may include where the information is contained in:

(a) a psychiatric report (e.g., student exhibits anti-social behaviour);

(b) a psychometric test (e.g., indicating that the student has the mental capacity of a 9 year old when the student is 15 years old);

(c) a confidential communication between the School and a parent about their child who is a student of the School; and

(d) Scholarship exam results, internal marks and teachers' notes.

10.25 Where access to the information may adversely impact on the student, the School might consider whether APP 12 permits the restriction or refusal of access, such as where:

(a) providing access would have an unreasonable impact on the privacy of others (APP 12.3(b));

(b) denying access is authorised by law (APP 12.3(g)); and

(c) providing access would reveal evaluative information generated with the School in connection with a commercially sensitive decision-making process (APP 12.3(j)). Where a School refuses to give access on this basis, it may include an explanation for the commercially sensitive decision in the reasons for the refusal.

10.26 If a parent of the student seeking access does not consent to their child having access, this should also be considered.

Do's and Don'ts

DO allow individuals to have access to, and copies of, their personal information, except where there are reasons to refuse access.

DO verify the identity of any individual seeking access to personal information.

DO respond to the request for access within a reasonable period of time.

DO inform people of their right to request access to their information. This should be done when collecting personal information.

DO consider the following matters when an access request is made:

- what information the individual wants access to;
- whether the School is permitted to refuse or restrict access;
- that there are various forms of access, including allowing the individual to inspect or take notes of the information, providing photocopies of the information, and giving the individual an accurate summary of the information;
- whether access can be given through the use of a mutually agreed intermediary;
- whether to charge the individual for the cost to the School of providing access. Any charge must not be excessive and the individual must not be charged for making the request.

DON'T provide an individual with direct access to information if that access would unreasonably impact on the privacy of others or reveal a commercially sensitive decision-making process. Instead, **DO** consider whether an alternative form of access can be provided.

DON'T refuse an individual access to their personal information just because it may be costly, inconvenient or difficult to provide access.

11. CORRECTION

11.1 If a School holds personal information and either

(a) the School is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(b) the individual requests the School to correct the information,

the School must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading (APP 13.1).

11.2 If the School corrects personal information about an individual that the School previously disclosed to another entity, and the individual requests that other entity be notified of the correction, then the School must take such steps (if any) as are reasonable in the circumstances to give that notification, unless it is impracticable or unlawful to do so (APP 13.2).

11.3 Where correction is denied, the School must give written notice of the reasons for refusal (except where unreasonable to set that out) and the mechanisms available to complain about the refusal (APP 13.3).

11.4 If the School refuses to correct the information and the individual requests the School to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, then the School must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information (APP 13.4).

11.5 If a request is made under APP 13.1 or APP 13.4, the School must respond to the request within a reasonable period after the request is made, and must not charge the individual for making the request, for correcting the information or for associating the statement with the information (APP 13.5).

Comment

11.6 General obligation

The principle is not intended to create a broad obligation on entities to maintain the correctness of personal information it holds at all times. The individual must either request correction, or there must be some other circumstance indicating that the information is incorrect (for example, if the School discovers an inconsistency during normal business practices or is notified by another entity that the information is incorrect). The principle will interact with APP 10 (quality of personal information) so that when the quality of personal information is assessed at the time of use or disclosure, the School may need to correct the information prior to that use or disclosure where it is satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

11.7 'Reasonable steps' to correct and notify of correction

If personal information is held for a range of purposes, and it is considered incorrect with regard to one of those purposes, the obligation to take reasonable steps to correct the information should apply.

11.8 Where a School corrects the personal information of an individual, it will be required to take reasonable steps to notify any other entity to which it had previously disclosed the information, if that notification is requested by the individual. The compliance burden will be reduced by the proviso that notification is not required if it would be impracticable or unlawful.

11.9 Statement relating to information

If a School refuses to correct personal information in response to an individual's request, APP 13.4 provides a mechanism for individuals to request that a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading be associated with the information. The School must take reasonable steps to associate with the personal information a statement so that it is apparent to users of the personal information that the individual has sought correction of that information. This will ensure that individuals retain control of how their personal information is handled. The statement should address matters relevant to the information being inaccurate, out-of-date, incomplete, irrelevant or misleading, and should not be unreasonably lengthy. The appropriate content and length of any statement will depend on the circumstances of the matter.

11.10 Time periods

A School must respond to correction requests within a reasonable period after the request is made. It is intended that a 'reasonable period' relating to more complicated requests will not usually exceed 30 days.

How to comply

11.11 The School should establish a standard procedure where, at the time of use or disclosure of information, it assesses the quality of that information and whether it may need to correct that information if it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

11.12 The School should also consider what steps are reasonable in the circumstances to correct information where the individual requests it to be corrected, to ensure that information is accurate, up-to-date, complete, relevant and not misleading.

11.13 However, if there is a disagreement as to whether an individual's information is accurate, complete, up-to-date, relevant and not misleading and if the individual requests it, the School must take such steps as are reasonable in the circumstances to associate a statement about the individual's claim with the information.

11.14 The School should also implement practices, systems and procedures to enable the School to deal with inquiries and complaints about its compliance with the correction provisions.

Do's and Don'ts

DO assess the information you use and disclose, and correct it if necessary to ensure it is accurate, up-to-date, complete, relevant and not misleading.

DO consider what steps are reasonable in the circumstances to correct information upon request by the individual.

DO encourage individuals to notify the School if they consider the personal information held about them is inaccurate, out-of-date, incomplete, irrelevant or misleading.

DO inform people of their right to correct their information. This should be done when collecting personal information.

DON'T refuse to correct personal information just because it may be costly, inconvenient or difficult to do so.

PART E

Annexure 1 – Summary of Mandatory Notification of Eligible Data Breaches

Annexure 2 - Template Data Breach Response Plan

Annexure 3 – Data Breach Risk Assessment Factors

Annexure 4 – Privacy Planning Template

Annexure 5 – Sample Privacy Policies

Annexure 6 – Sample Collection Notices

Annexure 7 - Permission to share personal information (including photos/videos) for promotional and other purposes

Annexure 8 – Short Form Disclosure Statement to Students

Annexure 9 - Short Form Disclosure Statement to Students Alternative (Sample Script for Counsellors)

Annexure 10 – Glossary of Terms

ANNEXURE 1 – SUMMARY OF MANDATORY NOTIFICATION OF ELIGIBLE DATA BREACHES

Maintain information governance and security – APP 1 and 11

Schools have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known Data Breach

Contain

Contain a suspected or known Data Breach where possible.

Assess

Schools will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the School has reasonable grounds to believe this is the case, then this is an **EDB** and it must notify individuals affected and the Information Commissioner. If it only has grounds to suspect that this is the case, then it must **conduct** an assessment. As part of the assessment, Schools should consider whether **remedial action** is possible.

Schools should consider adopting the OAIC's suggested a three-stage process:

- **Initiate**: plan the assessment and assign a response team or person
- **Investigate**: gather relevant information about the incident to determine what has occurred
- **Evaluate**: make an evidence-based decision about whether serious harm is likely (and document this).

Schools should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, a School should take steps to reduce any potential harm to individuals. For example, this might involve taking action to recover lost information before it is accessed or changing access controls on accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and Schools can progress to the review stage.

YES — **Is serious harm still likely?** — **NO**

Notify

Where serious **harm is likely**, a School must prepare a statement for the Commissioner (a form available on OAIC website) that contains:

- the School's identity and contact details
- a description of the Data Breach the kind/s of information concerned
- recommended steps for individuals affected.

Schools must also notify affected individuals, and inform them of the contents of this statement.

There are three options for notifying:

- **Option 1**: Notify all individuals
- **Option 2**: Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3**: publish the statement on the School's website and publicise it.

Schools can provide further information in their notification, such as an apology and an explanation of what they are doing about the Data Breach. **In some limited circumstances, an exception to the obligation to notify the individuals or the Commissioner may apply.**

Review

Review the incident and take action to prevent future Data Breaches. This may include:

- Fully investigating the cause of the Data Breach
- Developing a prevention plan
- Conducting audits
- Updating security/ response plan
- Considering changes to policies and procedures
- Revising staff training practices

Schools should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- other external or third parties (e.g. the ATO)
- The Australian Cyber Security Centre and related agencies professional bodies
- Credit card companies or financial services providers

Schools that operate outside Australia may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

This summary is a modified version of the OAIC Data Breach response summary available at https://www.oaic.gov.au/privacy/notifiable-data-breaches

ANNEXURE 2 - TEMPLATE DATA BREACH RESPONSE PLAN

Introduction

The template plan sets out the procedure to manage a School's response to the actual or suspected unauthorised access to or disclosure or loss of personal information (**Data Breach**). The School will need to adapt this template to their circumstances and may also wish to seek guidance from the Catholic Education Office, the Catholic Education Commission or equivalent (e.g., CSNSW), or the Association of Independent Schools to which they belong. In particular, it is likely that each Catholic Education Office will prepare their own tailored data breach response plan that covers all their schools. Before using this template, Catholic Schools should first consult their Catholic Education Office. This template can be used if the School's Catholic Education Office has not prepared its own data breach response plan.

Further guidance about responding to a Data Breach and an eligible data breach (EDB) under the notifiable data breaches scheme (**NDB Scheme**) is contained in Section 1 of Part B of this Manual

The OAIC has also published a '*Guide to developing a data breach response plan*', which can be of assistance to Schools when preparing a plan.[10]

Response plan

In the event of a Data Breach, School personnel must adhere to the four phase process set out below (as described in the Office of the Australian Information Commissioner's (**OAIC**) *Notifiable Data Breaches scheme: Resources for agencies and organisations.* It is important that appropriate records and any evidence are kept of the Data Breach and the response. Legal advice should also be sought if necessary.

Phase 1. Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The School personnel who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify [insert name of appropriate person]. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.
2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.
3. [insert name of appropriate person (as per 1)] must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.
4. Where a **High Risk** incident is identified, [insert name of appropriate person (as per 1)] must consider if any of the affected individuals should be notified immediately where serious harm is likely.
5. [insert name of appropriate person (as per 1)] must escalate **High Risk** and **Medium Risk** Data Breaches to the response team (whose details are set out at the end of this protocol).
6. If there could be media or stakeholder attention as a result of the Data Breach, it must be escalated to the response team.

[10]Available here https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/guide-to- developing-a-data-breach-response-plan.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g., where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

Phase 2. Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Data Breach and mitigate or remediate harm to affected individuals.
2. The response team is to work to evaluate the risks associated with the Data Breach, including by:
    a. identifying the type of personal information involved in the Data Breach;
    b. identifying the date, time, duration, and location of the Data Breach;
    c. establishing who could have access to the personal information;
    d. establishing the number of individuals affected; and
    e. establishing who the affected, or possibly affected, individuals are.
3. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an EDB.
4. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.
5. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

Phase 3. Consider Data Breach notifications

6. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.
7. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the OAIC.
8. After completing the statement, unless it is not practicable, the response team must

also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.

9. If it is not practicable to notify some or all of these individuals, the response team must publish the statement on their website, and take reasonable steps to otherwise publicise the contents of the statement to those individuals.

Phase 4. Take action to prevent future Data Breaches

10. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.
11. [insert name of relevant person] must enter details of the Data Breach and response taken into a Data Breach log. [insert name of relevant person] must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
12. [insert name of relevant person] must conduct a post-breach review to assess the effectiveness of the School's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.
13. [insert name of relevant person] must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.
14. [insert name of relevant person] must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

Response Team

[Insert current list of team members which clearly articulates their roles, responsibilities and authorities as well as their contact details. Each role should have a second contact point in case the first is not available. The team may include, for example, members of the IT department, human resources, legal and the Principal.

ANNEXURE 3 – DATA BREACH RISK ASSESSMENT FACTORS

Consider who the personal information is about	
Who is affected by the breach?	Are students, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.
Consider the kind or kinds of personal information involved	
Does the type of personal information create a greater risk of harm?	Some information, such as sensitive information (e.g., health records) or permanent information (e.g., date of birth) may pose a greater risk of harm to the affected individual(s) if compromised. A combination of personal information may also pose a greater risk of harm.
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	For example, a disclosure of a list of the names of some students who attend the School may not give rise to significant risk. However, the same information about students who have attended the School counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and address of students or parents would also create more significant risks.
Who has gained unauthorised access to the affected information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher at another school gains unauthorised access to a student's name, address and grades without malicious intent (e.g., if the information is accidentally emailed to the teacher), the risk of serious harm to the student may be unlikely.
Have there been other breaches that could have a cumulative effect?	A number of minor, unrelated breaches that might not, by themselves, create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches is considered. This could involve incremental breaches of the same School database, or known breaches from multiple different sources (e.g., multiple schools or multiple data points within the one school).
How could the personal information be used?	Consider the purposes for which the information could be used. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual and social or workplace bullying)? For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents. What is the risk of harm to the individual if the compromised information can be easily combined with other compromised or publicly available information?

Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	What is the risk of further repeat access, use or disclosure, including via mass media or online?
Is there evidence of intention to steal the personal information?	For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in way that renders it unusable if breached. If so, the risk of harm to the individual may be lessened.
What was the source of the breach?	For example, was it external or internal? Was it malicious or unintentional? Did it involve malicious behaviour or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information lost or stolen? Where the breach is unintentional or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.
Has the personal information been recovered?	For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?
What steps have already been taken to mitigate the harm?	Has the School fully assessed and contained the breach by, for example, replacing comprised security measures such as passwords? Are further steps required? This may include notification to affected individuals.
Is this a systemic problem or an isolated incident?	When identifying the source of the breach, it is important to note whether similar breaches have occurred in the past. If so, there may be a systemic problem with system security, or there may be more information affected than first thought, potentially heightening the risk.

Establish the cause and extent of the breach	
How many individuals are affected by the breach?	If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response must be proportionate. Although it is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.
Assess the risk of harm to the affected individuals	
Who is the information about?	Some individuals are more vulnerable and less able to take steps to protect themselves (e.g. younger students, students with disabilities/ special needs, vulnerable families/parents)
What kind or kinds of information is involved?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) or a combination of personal information may pose a greater risk of harm to the affected individual(s) if compromised.
How sensitive is the information?	The sensitivity of the information may arise due to the kind of information involved, or it may arise due to the context of the information involved. For example, a list of the names of some students who attend the School may not be sensitive information. However, the same information about students who have attended the School counsellor or students with disabilities.
Is the information in a form that is intelligible to an ordinary person?	Examples of information that may not be intelligible to an ordinary person, depending on the circumstances may include: (i) encrypted electronic information; (ii) information that the School could likely use to identify an individual, but that other people likely could not (such as a student number that only the School uses – this should be contrasted to a student number that is used on public documents); and (iii) information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).
If the information is not in a form that is intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?	For example, encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the breach. Even where none of these concerns apply, the School may need to consider the likelihood of the encryption algorithm being broken in the long term.
Is the information protected by one or more security measures?	For example, are the systems on which the information is stored protected by intrusion detection and prevention systems, which identified the attack and stopped the attacker from accessing any information or copying the information?

Assess the risk of harm to the affected individuals	
If the information is protected by one or more security measures, what is the likelihood that any of those security measures could be overcome?	For example, could an attacker have overcome network security measures protecting personal information stored on the network?
What persons (or kind of persons) have obtained or could obtain the information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a student's information without malicious intent, the risk of serious harm may be unlikely.
What is the nature of the harm that could result from the breach?	Examples include identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of business or employment opportunities, humiliation, damage to reputation or relationships, or workplace or social bullying or marginalisation. For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents.
In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?	Examples of steps that may remediate the serious harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorised practice, recovering records subject to unauthorised access or disclosure or loss, shutting down a system that was subject to unauthorised access or disclosure, or remotely erasing the memory of a lost or stolen device. Considerations about how quickly these steps are taken or the extent to which the steps taken are remediating harm will vary depending on the circumstances.
Any other relevant matters?	The nature of other matters that may be relevant will vary depending on the circumstances of the School and the Data Breach.
Assess the risk of other harms	
What other possible harms could result from the breach, including harms to the School or AIS/CEC (or equivalent to CEC in your State or Territory e.g., CSNSW)?	Examples include loss of public trust in the School or AIS/CEC (or equivalent), damage to reputation, loss of assets (e.g. stolen laptops), financial exposure (e.g., if bank account details are compromised), regulatory penalties (e.g., for breaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.

ANNEXURE 4 – PRIVACY PLANNING TEMPLATE

PERSONAL INFORMATION TEMPLATE - Student

Summary of Personal Information (PI) collected	Needed for a function or activity of School?	From whom is the PI collected?	Where is the PI recorded?	Who can access each class of information?	How long kept?	Level of security risk[11]	Disclosed outside School?
KEY:	Y/N	PA=Parent PU=Student SM=Staff member HP=Health Provider OR=Other (specify)	P=Paper file E=Electronic database	PR=Principal LS=Limited staff AS=All staff OR=Other (specify)	A=While student enrolled B=Up to 6 years after student leaves C=Up to 10 years after student leaves D=up to 23 years from date of incident E=Indefinite	H=High M=Medium L=Low	Y/N
Name							
Address							
Phone number(s)							
Date of birth (& age)							
Birth certificate							
Religion							
Parish information							
Conduct reports							
Next of kin							
Emergency contact numbers							
Names of doctors							
School reports							
Assessments							
Referrals[12]							

[11]Considering the nature of the information, type of storage, access and possible disclosure

[12]For example, government welfare agencies/departments.

ANNEXURE 4 – PRIVACY PLANNING TEMPLATE

PERSONAL INFORMATION TEMPLATE - Student

Summary of Personal Information (PI) collected	Needed for a function or activity of School?	From whom is the PI collected?	Where is the PI recorded?	Who can access each class of information?	How long kept?	Level of security risk[11]	Disclosed outside School?
Details of disability							
Court Orders							
Counselling reports							
Complaint records							
Communication with parents/carers							
Behaviour notes							
Previous school							
Health fund details							
Medicare number							
Medical reports							
File notes							
Diary entries							
Absence notes							
Case management notes							
Photos, video							
Employment information							
Legal case files							

ANNEXURE 4 – PRIVACY PLANNING TEMPLATE

PERSONAL INFORMATION TEMPLATE - Parent

Summary of Personal Information (PI) collected	Needed for a function or activity of School?	From whom is the PI collected?	Where is the PI recorded?	Who can access each class of information?	How long kept?	Level of security risk[13]	Disclosed outside School?
KEY:	Y/N	PA=Parent PU=Student SM=Staff member HP=Health Provider OR=Other (specify)	P=Paper file E=Electronic database	PR=Principal LS=Limited staff AS=All staff OR=Other (specify)	A=While student enrolled B=Up to 6 years after student leaves C=Up to 10 years after student leaves D=up to 23 years from date of incident E=Indefinite	H=High M=Medium L=Low	Y/N
Name							
Address							
Phone number(s)							
Date of birth (& age)							
Birth certificate							
Religion							
Parish information							
Emergency contact numbers							
Details of disability							
Court Orders							
Counselling reports							
Complaint records							
Communication with parents/carers							

[13] Considering the nature of the information, type of storage, access and possible disclosure

ANNEXURE 4 – PRIVACY PLANNING TEMPLATE

PERSONAL INFORMATION TEMPLATE - Parent

Summary of Personal Information (PI) collected	Needed for a function or activity of School?	From whom is the PI collected?	Where is the PI recorded?	Who can access each class of information?	How long kept?	Level of security risk[13]	Disclosed outside School?
Health fund details							
Medicare number							
Medical reports							
File notes							
Diary entries							
Absence notes							
Case management notes							
Photos, video							
Employment information							
Volunteering information							
Legal case files							
Unsolicited information							

ANNEXURE 5 – SAMPLE PRIVACY POLICIES

Introduction

Further guidance on privacy policies is contained in Section 1 of Part C and Section 1 of Part D.

The sample privacy policies are samples only and must be adapted to reflect each School or system's particular acts and practices. In particular, Schools' use of AI is evolving. Each School and system should consider their own use of AI and ensure it is adequately addressed in their privacy policy.

Sample Privacy Policy – AIS Schools

[School name] Privacy Policy

Date: [insert]

This Privacy Policy sets out how the School manages personal information and your rights in relation to your personal information, including how to complain and how we deal with complaints.

The School is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988* (**Privacy Act**). In relation to health records, the School is also bound by the [***insert relevant State/Territory legislation as follows*** [Health Privacy Principles which are contained in the *Health Records and Information Privacy Act 2002* (NSW) (**Health Records Act**)][Health Privacy Principles which are contained in the *Health Records Act 2001* (Vic) (**Health Records Act**)][Privacy Principles which are contained in the *Health Records (Privacy and Access) Act 1997* (ACT) (**Health Records Act**)]].

Under the Privacy Act [***insert the following in NSW***: and the Health Records Act], the Australian Privacy Principles [***insert the following in NSW***: and Health Privacy Principles] do not apply to certain treatment of an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record held by the School, where the treatment is directly related to a current or former employment relationship between the School and the employee.[***insert for Vic and ACT*** The School handles staff health records in accordance with the [Health ***insert 'Health' for Vic only***] Privacy Principles in the Health Records Act.]

The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment. The current version of this Privacy Policy is published on our website.

Kinds of personal information we collect

The types of information the School collects includes (but is not limited to) personal information, including health and other sensitive information, about:

- students and parents and/or guardians ('**Parents**') before, during and after the course of a student's enrolment at the School, including: [***insert the following as relevant, and add any other general kinds of information (including any personal information collected by or generated through the use of an AI system)***]
    - » name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;

  - » parents' education, occupation, language spoken at home, nationality and country of birth;
  - » health information (e.g., details of disability and/or allergies, dietary requirements, absence notes, immunisation details, medical reports and names of doctors);
  - » results of assignments, tests and examinations;
  - » conduct and complaint records, or other behaviour notes, and school reports;
  - » information about referrals to government welfare agencies;
  - » counselling reports;
  - » health fund details and Medicare number;
  - » any Family Court orders;
  - » criminal records;
  - » volunteering information; and
  - » photos and videos at School events;
- job applicants, volunteers and contractors, including: [***insert the following as relevant, and add any other general kinds of information (including any personal information collected by or generated through the use of an AI system)***]
  - » name, contact details (including next of kin), date of birth, and religion;
  - » information on job application;
  - » professional development history;
  - » salary and payment information, including superannuation details;
  - » health information (e.g., details of disability and/or allergies, and medical certificates);
  - » complaint records and investigation reports;
  - » leave details;
  - » photos and videos at School events;
  - » workplace surveillance information; and
  - » work emails and private emails (when using work email address) and Internet browsing history; and
- other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.

How we collect personal information

Personal information you provide: The School generally collects personal information about an individual directly from the individual (or their Parent in the case of students). This includes by way of forms, face-to-face meetings and interviews, emails and telephone calls.

***Personal information provided by other people*:** In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional, a reference from another school or a referee for a job applicant. If a student transfers to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.

[***Personal information generated by artificial intelligence (AI) systems:*** We might also collect personal information by using AI systems to generate it. The kinds of personal information that may be generated by AI systems include those set out above under the heading 'Kinds of personal information we collect'.]**

Personal information from other sources: We may also collect personal information through surveillance activities (such as CCTV security cameras) and [student email monitoring].

Purposes for which we collect, use and disclose personal information

The purposes for which the School collects, uses and discloses personal information depend on our relationship with you and include the following:

Students and Parents:

- providing schooling and school activities;
- satisfying the needs of Parents, the needs of students and the needs of the School throughout the whole period a student is enrolled at the School;
- making required reports to government authorities;
- keeping Parents informed about matters related to their child's schooling, through correspondence, apps, newsletters and magazines;
- day-to-day administration of the School;
- looking after students' educational, social and health wellbeing;
- seeking donations for the School (see the 'Fundraising' section of this Privacy Policy); and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

[***Note: If personal information will be used for training the School's AI systems (or for other purposes associated with AI systems not already listed here), then that should be listed here (and below if the personal information includes that of volunteers, job applicants and/or contractors). However, training AI systems is potentially a high risk activity, particularly in relation to student personal information, and the School should consider seeking further advice (including in relation to the wording of this policy).***]

Volunteers:

- to contact you about, and administer, the volunteer position;
- for insurance purposes; and
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Job applicants and contractors:

- assessing and (if successful) engaging the applicant or contractor;
- administering the individual's employment or contract;
- [seeking donations for the School (see the 'Fundraising' section of this Privacy Policy);]**
- for insurance purposes; and
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

[***Note: In respect of the following section 'Automated decision making', see the guidance on this in paragraphs 1.2 and 1.7 of Part C of this Manual.***]

****[Automated decision making**

We use personal information in the operation of computer programs to make, or assist us in making, certain decisions **(automated decisions)**. The personal information we use for this purpose is ***[insert kinds of personal information used in making the decisions set out below]***. The decisions we make using this personal information in the operation of computer programs, are as follows:

- [***insert types of decisions, noting that you only need to include those that could reasonably be expected to significantly affect the rights or interests of an individual, and where that information is used in the operation of a computer program (AI system) to make the decision or as a substantial input to the making of the decision e.g. whether a student has the prerequisite experience to participate in a particular course.***]; and
- other decisions as notified by us from time to time.]

Who we disclose personal information to

The School may disclose personal information, including sensitive information, for educational, care and administrative purposes, and to seek support and advice. This may include to:

- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
- [organisations that assist us with fundraising (see the 'Fundraising' section of this Privacy Policy);]
- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection, students with additional needs and for the purpose of administering Google Apps for Education and ensuring its proper use (see further the section below 'Sending and storing information overseas);
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes;
- people providing administrative and financial services to the School;
- [the provider of our information management and storage system and other information technology services;]**
- recipients of School publications, such as newsletters and magazines;
- students' parents or guardians;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

[***Note: If the School discloses personal information to a third party as part of the School's use of AI systems, this should be included in the list above. For example, 'third party providers of the AI systems we use'.***]

How we store personal information

We store your personal information in hard copy and electronically. [We use information management and storage systems provided by third party service providers. Personal information is stored with and accessible by the third party service providers for the purpose of providing services to the School in connection with the systems.]

The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information. See further the section below 'Sending and storing information overseas.'

Sending and storing information overseas

The School may disclose personal information about an individual to overseas recipients in certain circumstances, for instance, to facilitate a school exchange.

The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services and provide technical support. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.**

An example of such a cloud service provider is Google. Google provides the 'Google Apps for Education' (GAFE) including Gmail, and stores and processes limited personal information for this purpose. School personnel and the AIS and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g., instant messaging), documents and associated administrative data for the purposes of administering GAFE and ensuring its proper use.

**[*If GAFE is not applicable to your School, replace this paragraph with one relevant to the platform used by the School (e.g., Microsoft 365)*]

[***Note: If a School discloses personal information to a third party as part of the School's use of AI systems, and the third party (or its personnel) is located outside Australia, this (including the relevant countries) should be noted here. For example, 'The School uses AI systems that are provided by third parties. These third parties may store or have access to personal information input into, and/or generated by, these AI systems. These third parties may be located outside Australia, including in [insert countries].'***]

Fundraising *[If you also use or disclose personal information for direct marketing, this should be incorporated into this section (and the heading changed to 'Fundraising and marketing')]*

The School treats seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to provide a quality learning environment in which both students and staff thrive. Your personal information may be used to make an appeal to you. [It may also be disclosed to organisations that assist in the School's fundraising activities, for example, the School's Foundation or alumni organisation and, on occasions, external fundraising organisations].

If you do not want to receive fundraising communications from us, please [contact our Privacy Officer].

Security of personal information

The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

These steps include: [***Note: Only List steps that you are sure the School implements. Otherwise, this may be misleading.***]

- Restricting access to information on the School databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where personal and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures around the School buildings and grounds to prevent break-ins.
- Implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human recourses policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Access and correction of personal information

Under the Commonwealth Privacy Act [***insert the following for NSW, Vic and ACT***: and the Health Records Act], an individual has the right to seek access to, and/or correction of, any personal information which the School holds about them. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access, update or correct any personal information the School holds about you or your child, please contact the [School Principal] or [School Administrator] by email, post or telephone at [insert contact details]. The School may require you to verify your identity and specify what information you require. The School may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). If the information sought is extensive, the School will advise the likely cost in advance.

If we decide to refuse your request, we will provide you with written notice explaining the reasons for refusal (unless, in light of the grounds for refusing, it would be unreasonable to provide reasons) and how to complain.

Consent and rights of access to the personal information of students

The School respects every Parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. Generally,the School will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

Parents may seek access to personal information held by the School about them or their child by contacting the [School Principal] or [School Administrator] by telephone or in writing (details in the section above 'Access and correction of personal information'). However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where the School believes the student has capacity to consent and the School is not permitted to disclose the information to the Parent without the student's consent, where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Enquiries and complaints

If you would like further information about the way the School manages the personal information it holds, or wish to complain that you believe that the School has breached the Australian Privacy Principles [or the Health Privacy Principles] please contact the [School Principal] by email, post or telephone at [insert contact details here]. The School will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC) via the OAIC website, www.oaic.gov.au.

[***Legend***:

** If applicable]

Sample Privacy Policy – NCEC Schools

[Catholic Education Office of the [...] Diocese / ...System] Privacy Policy

Date: [insert]

This Privacy Policy applies to schools conducted by the [Catholic Education Office of the [Diocese (CEO) / System]] and sets out how [the **CEO** / System] and each school manages personal information and your rights in relation to your personal information, including how to complain and how we deal with complaints. [Each school is legally related to the CEO / System.]

The [CEO / System] and its schools are bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988* (**Privacy Act**). In relation to health records the [CEO / System] and its schools are also bound by the [***insert relevant State/ Territory legislation as follows*** [Health Privacy Principles contained in the *Health Records and Information Privacy Act 2002* (NSW) (**Health Records Act**)][Health Privacy Principles which are contained in the *Health Records Act 2001* (Vic) (**Health Records Act**)][Privacy Principles which are contained in the *Health Records (Privacy and Access) Act 1997* (ACT) (**Health Records Act**)]].

Under the Privacy Act [***insert the following in NSW:*** and the Health Records Act], the Australian Privacy Principles [***insert the following in NSW:*** and Health Privacy Principles] do not apply to certain treatment of an employee record. As a result, this Privacy Policy does not apply to the school's treatment of an employee record held by the school, where the treatment is directly related to a current or former employment relationship between the school and the employee. [***insert for Vic and ACT*** The school handles staff health records in accordance with the Privacy Principles in the Health Records Act.]

The [CEO / System] may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to schools' operations and practices and to make sure it remains appropriate to the changing school environment. The current version of this Privacy Policy is published on our website.

Kinds of personal information we collect

The types of information schools collect includes (but is not limited to) personal information, including health and other sensitive information, about:

- students and parents and/or guardians (**Parents**) before, during and after the course of a student's enrolment at the school [***insert the following as relevant, and add any other general kinds of information (including any personal information collected by or generated through the use of an AI system)***]
  - » name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
  - » parents' education, occupation, language spoken at home, nationality and country of birth;
  - » health information (e.g., details of disability and/or allergies, dietary requirements, absence notes, immunisation details, medical reports and names of doctors);
  - » results of assignments, tests and examinations;
  - » conduct and complaint records, or other behaviour notes, and school reports;
  - » information about referrals to government welfare agencies;
  - » counselling reports;
  - » health fund details and Medicare number;
  - » any Family Court orders;
  - » criminal records;
  - » volunteering information; and
  - » photos and videos at school events;
- job applicants, volunteers and contractors, including: [***insert the following as relevant, and add any other general kinds of information (including any personal information collected by or generated through the use of an AI system)***]
  - » name, contact details (including next of kin), date of birth, and religion;
  - » information on job application;
  - » professional development history;
  - » salary and payment information, including superannuation details;
  - » health information (e.g. details of disability and/or allergies, and medical certificates);
  - » complaint records and investigation reports;

  - » leave details;
  - » photos and videos at school events;
  - » workplace surveillance information; and
  - » work emails and private emails (when using work email address) and Internet browsing history; and
- other people who come into contact with the school, including name and contact details and any other information necessary for the particular contact with the school.

How we collect personal information

Personal information you provide: A school will generally collect personal information about an individual directly from the individual (or their Parent in the case of students). This includes by way of forms, face-to-face meetings and interviews, emails and telephone calls. A school also collects personal information when a student uses their issued Compass Card (which records attendance and the use of library and ICT services).

Enrolment applications within the diocese: If an enrolment application is made to two (or more) schools in the same diocese, the personal information provided during the application stage may be shared between the schools. This personal information may include health information and is used for the purpose of considering and administering the enrolment of the student within the diocese.

Personal information provided by other people: In some circumstances a school may be provided with personal information about an individual from a third party, for example a report provided by a medical professional, a reference from another school or a referee for a job applicant. If a student transfers to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.

[***Personal information generated by artificial intelligence (AI) systems: We might also collect personal information by using AI systems to generate it. The kinds of personal information that may be generated by AI systems include those set out above under the heading 'Kinds of personal information we collect'.***]**

Personal information from other sources: We may also collect personal information through surveillance activities (such as CCTV security cameras) and [student email monitoring].

Purposes for which we collect, use and disclose personal information

The purposes for which [the CEO / System] and a school collects, uses and discloses personal information depend on our relationship with you and include the following:

Students and Parents

- providing schooling and school activities;
- satisfying the needs of Parents, the needs of students and the needs of the school throughout the whole period a student is enrolled at the school;
- making required reports to government authorities;
- keeping Parents informed about matters related to their child's schooling, through correspondence, apps, newsletters and magazines;
- day-to-day administration, including seeking the payment of fees for schools within the same diocese when a student transfers between such schools;
- looking after students' educational, social, spiritual and health wellbeing;

- seeking donations for the school (see the 'Fundraising' section of this Privacy Policy); and
- to satisfy the [CEO's / System's] and the school's legal obligations and allow the school to discharge its duty of care.

[***Note: If personal information will be used for training a school's (and/or the CEO's / System's) AI systems (or for other purposes associated with AI systems not already listed here), then that should be listed here (and below if the personal information includes that of volunteers, job applicants and/or contractors). However, training AI systems is potentially a high risk activity, particularly in relation to student personal information, and you should consider seeking further advice (including in relation to the wording of this policy).***]

Volunteers:

- to contact you about, and administer, the volunteer position;
- for insurance purposes; and
- satisfying the [CEO's / System's] and the school's legal obligations, for example, in relation to child protection legislation.

Job applicants and contractors:

- assessing and (if successful) engaging the applicant or contractor;
- administering the individual's employment or contract;
- [seeking donations for the relevant school (see the 'Fundraising' section of this Privacy Policy);]
- for insurance purposes; and
- satisfying the [CEO's / System's] and the school's legal obligations, for example, in relation to child protection legislation.

[***Note: In respect of the following section 'Automated decision making', see the guidance on this in paragraphs 1.2 and 1.7 of Part C of this Manual.***]

****[Automated decision making**

[A school][the CEO / System] might use personal information in the operation of computer programs to make, or assist us in making, certain decisions **(automated decisions)**. The personal information we use for this purpose is ***[insert kinds of personal information used in making the decisions set out below]***. The decisions we make using this personal information in the operation of computer programs, are as follows:

- [***insert types of decisions, noting that you only need to include those that could reasonably be expected to significantly affect the rights or interests of an individual, and where that information is used in the operation of a computer program (AI system) to make the decision or as a substantial input to the making of the decision e.g. whether a student has the prerequisite experience to participate in a particular course.***]; and
- other decisions as notified by us from time to time.]

Who we disclose personal information to

A school may disclose personal information, including sensitive information, for educational, care and administrative purposes, and to seek support and advice. This may include to:

- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student, and schools within the same diocese where concurrent applications for enrolment are made to those schools;
- government departments (including for policy and funding purposes);
- the CEO, the [Catholic Education Commission (**CEC**)][***insert equivalent to CEC if CEC not applicable to your State/Territory, e.g., CSNSW***], the school's Diocese/Archdiocese and the parish, other related church agencies/entities, and schools within other Dioceses/other Dioceses;
- the school's local parish;
- medical practitioners;
- people providing educational, support and health services to the school, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
- [organisations that assist us with fundraising (see the 'Fundraising' section of this Privacy Policy);]
- providers of specialist advisory services and assistance to the school, including in the area of Human Resources, child protection and students with additional needs;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- agencies and organisations to whom we are required to disclose personal information for education and research purposes;
- people and organisations providing administrative, technology and financial services to the school;
- [the Catholic Education Network and other][providers of our information management and storage system and other information technology services;]**
- recipients of school publications, such as newsletters and magazines;
- students' parents or guardians;
- anyone you authorise the school to disclose information to; and
- anyone to whom we are required or authorised to disclose the information by law, including child protection laws.

[***Note: If a school (and/or the CEO / System) discloses personal information to a third party as part of the school's use of AI systems, this should be included in the list above. For example, 'third party providers of the AI systems our schools use'.***]

Exception in relation to related schools: The Privacy Act allows each school, being legally related to each of the other schools conducted by the [CEO / System] to share personal (but not sensitive) information with other schools conducted by the [CEO / System]. Other [CEO / System] schools may then only use this personal information for the purpose for which it was originally collected by the [CEO / System], a reasonably expected purpose that is related to the purpose for which it was originally collected by the [CEO / System], or another purpose that is permitted by the Privacy Act. This allows schools to transfer information between them, for example, when a student transfers from a [CEO / System] school to another school conducted by the [CEO / System].

How we store personal information

A school may store your personal information in hard copy and electronically.

[***insert the following if applicable][Storage and access as part of centralised information systems:*** The school uses centralised information management and storage systems (**Systems**). These Systems are provided by the Catholic Education Network (**CEnet**) and third party service providers. CEnet is owned by the Catholic Dioceses. Personal information is stored with and accessible by CEnet and the third party service providers for the purpose of providing services to the School in connection with the Systems and for CEnet, administering the education of students.] [***The following is an alternative paragraph for Schools that use information management and storage systems provided by third parties, but not CEnet***] [***Storage and access as part of [centralised] information systems*** The School uses [centralised] information management and storage systems (**Systems**) provided by third party service providers. Personal information is stored with and accessible by the third party service providers for the purpose of providing services to the School in connection with the Systems.]

A school may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information. See further the section below 'Sending and storing information overseas.'

Sending and storing information overseas

A school may disclose personal information about an individual to overseas recipients in certain circumstances, for instance, to facilitate a school exchange.

The school may use other online or 'cloud' service providers to store personal information and to provide online services to the school that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services and provide technical support. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.**

An example of such a cloud service provider is Google. Google provides the 'Google Apps for Education' (GAFE) including Gmail, and stores and processes limited personal information for this purpose. School personnel, the CEO, the [CEC][***insert equivalent to CEC if CEC not applicable to your State/Territory***] and their service providers [including CEnet] may have the ability to access, monitor, use or disclose emails, communications (e.g., instant messaging), documents and associated administrative data for the purposes of administering GAFE and ensuring its proper use.

** [***If GAFE is not applicable to your Diocese / System, replace this paragraph with one relevant to the platform used by the Diocese / ...System(e.g., Microsoft 365)***]

[***Note: If a school (and/or the CEO / System) discloses personal information to a third party as part of the school's use of AI systems, and the third party (or its personnel) is located outside Australia, this (including the relevant countries) should be noted here. For example, 'Our schools use AI systems that are provided by third parties. These third parties may store or have access to personal information input into, and/or generated by, these AI systems. These third parties may be located outside Australia, including in [insert countries].'***]

Fundraising *[If a school also uses or discloses personal information for direct marketing, this should be incorporated into this section (and the heading changed to 'Fundraising and marketing')]*

Schools treat seeking donations for the future growth and development of the school as an important part of ensuring that the school continues to be a quality learning environment in which both students and staff thrive. Your personal information may be used to make an appeal to you. [It may also be disclosed to an organisation that assists in the school's fundraising activities, for example, the school's Foundation or alumni organisation and, on occasions, external fundraising organisations].

If you do not want to receive fundraising communications from the [CEO / System] or school, please [contact our Privacy Officer].

Security of personal information

Each school has in place steps to protect the personal information the school holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

These steps include: ***[Note: Only List steps that you are sure each school implements. Otherwise, this may be misleading.]***

- Restricting access to information on the School databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where personal and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures around the School buildings and grounds to prevent break-ins.
- Implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human recourses policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Access and correction of personal information

Under the Commonwealth Privacy Act [***insert the following for NSW, Vic and ACT:*** and Health Records Act], an individual has the right to seek access to, and/or correction of, any personal information which the [CEO / System] or a school holds about them. There are some exceptions to this right set out in the Act.

Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access, update or correct any personal information the [CEO / System] or a school holds about you or your child, please contact the [school's Principal] or [school's Administrator] by email, post or telephone at [insert contact details].

The school may require you to verify your identity and specify what information you require. The school may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). If the information sought is extensive, the school will advise the likely cost in advance.

If we decide to refuse your request, we will provide you with written notice explaining the reasons for refusal (unless, given the grounds for refusal, it would be unreasonable to provide reasons) and how to complain.

Parents can also log on to the Compass Parent Portal and correct and update some of their or their child's personal information at any time.

Consent and rights of access to the personal information of students

The [CEO / System] respects every Parent's right to make decisions concerning their child's education.

Generally, a school will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. Generally, a school will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

Parents may seek access to personal information held by a school or the [CEO / System] about them or their child by contacting the [school' Principal] or [school's Administrator] by telephone or in writing (details in the section above 'Access and correction of personal information'). However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where the school believes the student has capacity to consent and the school is not permitted to disclose the information to the Parent without the student's consent, where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the student.

A school may, at its discretion, on the request of a student grant that student access to information held by the school about them, or allow a student to give or withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Enquiries and complaints

If you would like further information about the way the [CEO / System] or a school manages the personal information it holds, or wish to complain that you believe that [the CEO / System] or a school has breached the Australian Privacy Principles [or the Health Privacy Principles], please contact the [school's Principal] by email, post or telephone at [insert contact details here]. The [CEO / System] or the school will investigate any complaint and will notify you of a decision in relation to your complaint as soon as is practicable after it has been made.

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC) via the OAIC website, www.oaic.gov.au.

[***Legend***:

** If applicable]

ANNEXURE 6 – SAMPLE COLLECTION NOTICES

The notices below are examples only. They should be adapted to suit the situation of each School. Further information about the notices is contained in Section 1 of Part C of this Manual.

The notices below contain example information for a School's use of AI systems. School's use of AI systems is evolving. Each School should consider their own use of AI systems and ensure it is adequately addressed in the applicable privacy notice. Depending on how a School uses AI systems, it may need to consider providing individuals with a specific collection notice for the School's use of AI systems.

Standard Collection Notice (for parents and students)

The standard collection notice below is designed to ensure students and parents are aware of a School's handling of their personal information during the course of the student's enrolment at the School. Schools could consider including it in enrolment forms and in each student's school diary.

This standard collection notice will not be able to cover every situation where a School collects personal information and each School should consider (a) what types of information they usually collect and should cover and (b) whether additional collection notices need to be provided in particular situations at particular points in time. For example, a separate collection notice should be provided to VET (Vocational Education and Training) students as part of the enrolment process.

Sample Standard Collection Notice

This notice explains how the School handles the personal information of students and parents or guardians (together **you**). [***Note: insert the following as relevant (and adapt if necessary).***] The School is conducted by the [Catholic Education Office of the [ ] Diocese (**CEO**) / System]. References to the School (and we, our) include the CEO.]

How and Why does the School Collect Personal Information?

1. The School collects personal information about you before and during the course of a student's enrolment at the School. This may be in writing, through technology systems or in the course of conversations. [We might also use artificial intelligence (AI) systems to generate your personal information.**] [***Note: If the School collects personal information from a third party, or the individual may not be aware that the School collects certain personal information, include here the fact and circumstances of collection. For example: We may also collect personal information from third parties, such as …'***] The types of personal information the School collects includes sensitive information, which includes health information.
2. The primary purpose of collecting personal information is to enable the School to provide schooling to students enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable students to take part in all the activities of the School. [***Note: If personal information will be used for training the School's AI systems (or for other purposes associated with AI systems not already mentioned in the proceeding sentence), then that should be listed here. However, training AI systems is potentially a high risk activity, particularly in relation to student personal information, and the School should consider seeking further advice (including in relation to the wording of this notice).***]

3. The School has legal obligations which require certain information to be collected and disclosed. These include relevant Education Acts, and Public Health [and Child Protection]* laws [***Note: Insert any other applicable laws that require the personal information to be collected***], as well as the School's duty of care to students.
4. A student's enrolment may be delayed or prevented if the School cannot collect certain personal information. This is particularly so where the information is relevant to the health and safety of the student, other students and/or staff.
5. If you provide the School with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the School and why.

To Whom Does the School Disclose Information

6. The School may disclose your personal and sensitive information for educational, care and administrative purposes, and to seek support and advice. This may include to:
    - other schools and teachers at those schools, including a new School to which a student transfers to facilitate the transfer of the student, (see also para [12] below);
    - government departments (including for policy and funding purposes);
    - [Catholic Education Office, the Catholic Education Commission or equivalent (e.g., CSNSW), the School's Diocese/Archdiocese and the parish, other related church agencies/entities, and Schools within other Dioceses/other Dioceses;]*
    - medical practitioners;
    - people providing educational, support and health services to the School, including specialist visiting teachers, specialist advisors, [sports] coaches, volunteers, and counsellors;
    - [organisations that assist us with fundraising (see para [11] below)];
    - providers of learning and assessment tools;
    - assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
    - [the third party providers of our information management and storage systems (for the purpose of the providers providing services to the School in connection with the systems;]**
    - people providing other information technology services to the School (see also para [9] below)
    - people providing administrative and financial services to the School;
    - anyone you authorise the School to disclose information to; and
    - anyone to whom the School is required or authorised to disclose the information to by law, including child protection laws.

    [***Note: If the School discloses personal information to a third party as part of the School's use of AI systems, this should be included in the list above. For example, 'third party providers of the AI systems we use'.***]
7. Personal information collected from students is regularly disclosed to their parents or guardians.
8. School activities and news (including student achievements) are frequently published in the School's journals, newsletters and magazines, on our [insert name of school app – assuming it is accessible by parents, students and teachers only], on our intranet

or otherwise shared with the School community (current, future and past students, parents and teachers). This may include personal information (including photographs and videos) of students and parents involved in School activities such as academic and sporting events and achievements, concerts and plays, school camps and school excursions. The School will obtain permissions [annually] if we would like to include photographs or videos [or other identifying material] of students (or parents) in our promotional material or otherwise make this material available to the public such as on the internet.

9. [The School uses centralised information management and storage systems (**Systems**). These Systems are provided by the Catholic Education Network (**CEnet**) and third party service providers. CEnet is owned by the Catholic dioceses. Personal information is stored with and accessible by CEnet and the third party service providers for the purpose of providing services to the School in connection with the Systems and for CEnet, for administering the education of students.]***

Overseas Storage and/or Disclosure

10. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some personal information may be provided to these service providers to enable them to authenticate users that access their services, and for technical support. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of online or 'cloud' service providers is contained in the School's Privacy Policy.**

[***Note: If a School discloses personal information to a third party as part of the School's use of AI systems, and the third party (or its personnel) is located outside Australia, this (including the relevant countries) should be noted here. For example, 'The School uses AI systems that are provided by third parties. These third parties may store or have access to personal information input into, and/or generated by, these AI systems. These third parties may be located outside Australia, including in [insert countries].'***]

[***Note: If the School is likely to disclose personal information to overseas recipients, include that fact here, including the countries in which such overseas recipients are likely to be located (if practicable to specify), and the description of the overseas recipient.***]

Fundraising

11. The School may engage in fundraising activities. Your personal information may be used to make an appeal to you. [It may also be disclosed to organisations that assist in the School's fundraising activities solely for that purpose.] We will not disclose your personal information to third parties for their own marketing purposes without your consent.

Enrolment Applications with the Diocese

12. [If you make an enrolment application to another School within our Diocese, personal information provided during the application stage may be collected from, or shared with, the other School. This personal information may include sensitive information and is used for the purpose of considering and administering the enrolment of the student within the Diocese.]***

Your Rights and How to Complain

13. The School's Privacy Policy, accessible on the School's website, sets out how you can:

- seek access to and correction of your personal information which the School holds; and
- make a privacy complaint and how we will handle the complaint.

[***Legend:***

* As appropriate

** If applicable

*** Catholic schools only. This will not be applicable to all Catholic schools. Delete if not applicable.]

Employment Collection Notice (for job applicants)

When receiving employment applications an 'employment collection notice' should be sent to the individual with the acknowledgment. This notice could be worded as follows:

Sample Employment Application Collection Notice

1. In order to assess your application for employment, [name of School] collects your personal information. [***Note: insert any other purposes for which the personal information is collected. If personal information will be used for training the School's AI systems (or for other purposes associated with AI systems not already mentioned in the proceeding sentence), then that should be listed here. However, training AI systems is potentially a high risk activity and the School should consider seeking further advice (including in relation to the wording of this notice).***] If we cannot collect some of your personal information, we may be limited in our ability to assess your application.
2. We collect your personal information directly from you (including from your resume) [, as well as from other sources (such as your referees and the results of criminal background and working with children checks).*] [We might also use artificial intelligence (**AI**) systems to generate your personal information.*] We may keep your information on file if your application is unsuccessful in case another position becomes available.
3. [We are required to [conduct a criminal record check] collect information [regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences] under Child Protection laws.*]
4. [Note: Insert the following as applicable]We will not disclose your personal information to a third party without your consent unless otherwise permitted. / We may disclose your personal information to [insert list e.g., support vendors that provide services around staff administration systems]. [***Note: If the School discloses personal information to a third party as part of the School's use of AI systems, this should be included in the proceeding list. For example, 'third party providers of the AI systems we use'.***] [These third parties may be located outside Australia, including in ***insert countries if practicable to specify***.*]
5. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as email services. Some limited personal information may be provided to these service providers to enable them to authenticate users that access their services and provide technical support. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of on online or 'cloud' service providers is contained in the School's Privacy Policy.*
6. The School's Privacy Policy, accessible on the School's website, contains details of how you may seek access to and correction of your personal information which the School

holds, as well as how you can make a privacy complaint and how we will handle the complaint..

7. If you provide us with the personal information of others (e.g. referees), we encourage you to inform them that you are disclosing that information to the School and why.

[***Legend:***

* If applicable]

Comment

The APPs provide that personal information should be de-identified or destroyed when it is no longer needed. If Schools wish to retain a job applicant's information on file, in case another position becomes available, this should be included in the Collection Notice. The same applies to contractors.

If unsolicited job applications are received and the School wishes to retain the applicant's information, the 'employment collection notice' should be sent to them.

If you intend to pass on information to a related School, you should make the applicant aware of this in the 'employment collection notice'.

Contractor Collection Notice

In most circumstances, new contractors should be sent a modified version of the 'employment collection notice'. This notice could be worded as follows:

Sample Contractor Collection Notice

1. In order to assess your application to provide services to the School, and to administer our ongoing relationship with you, [name of School] collects your personal information. [***Note: insert any other purposes for which the personal information is collected. If personal information will be used for training the School's AI systems (or for other purposes associated with AI systems not already mentioned in the proceeding sentence), then that should be listed here. However, training AI systems is potentially a high risk activity and the School should consider seeking further advice (including in relation to the wording of this notice).***] If we cannot collect some of your personal information, we may be limited in our ability to assess your application or to permit you to continue providing services to us.
2. We collect your personal information directly from you (including from your resume) [, as well as from other sources (such as your referees and the results of criminal background and working with children checks).*] [We might also use artificial intelligence (**AI**) systems to generate your personal information.*]
3. [We are required to [conduct a criminal record check] collect information [regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences] under Child Protection law.*]
4. [Note: Insert the following as applicable]We will not disclose this information to a third party without your consent unless otherwise permitted. / We may disclose your personal information to [insert list e.g., support vendors that provide services around administration systems]. [***Note: If the School discloses personal information to a third party as part of the School's use of AI systems, this should be included in the proceeding list. For example, 'third party providers of the AI systems we use'.***] [These third parties may be located outside Australia, including in ***insert countries if practicable to specify***.*]

5. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may be provided to these service providers to enable them to authenticate users that access their services and provide technical support. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of an online or 'cloud' services provider is contained in the School's Privacy Policy.*
6. The School's Privacy Policy, accessible on the School's website, contains details of how you may seek access to and correction of your personal information which the School holds, as well as how you can make a privacy complaint and how we will handle the complaint.
7. If you provide us with the personal information of others (e.g. referees), we encourage you to inform them that you are disclosing that information to the School and why.

[***Legend:***

* If applicable]

ANNEXURE 7 - PERMISSION TO SHARE PERSONAL INFORMATION (INCLUDING PHOTOS/VIDEOS) FOR PROMOTIONAL AND OTHER PURPOSES

[Note: This form is explained in Sections 3.10 and 9.11 of Part C of this Manual.]

[NAME of SCHOOL]

PERMISSION TO SHARE PERSONAL INFORMATION

FOR PROMOTIONAL AND OTHER PURPOSES

Insert School logo here

Dear Parent/Guardian

Information/news about school achievements, activities, events and excursions (including those outside the school campus) often contains the personal information of students (and other individuals) involved in those activities and events, including photos and videos of students. This information is frequently published in the school's journals, newsletters and magazines, on our [insert name of school app accessible by parents, students and teachers only], [on our closed Facebook page that is only accessible to students and parents], on our intranet or otherwise shared with the School community (current, future and past students, parents and teachers [insert any other members of the School community]). The information may also be used in class activities and teacher development materials.

In this form we seek your consent to make personal information about your child available to the public, including to promote the school. The personal information is limited to your child's name, image, information about your child's participation in school activities and events (including achievements), [insert any other personal information].

[***Insert the following if relevant***] This form also seeks consent for [***insert relevant educational authority, e.g.: [name of system or School]/ Catholic Education Commission [or equivalent in your State or Territory***] [and the [xx] Diocese (Diocese)] to use photographs/videos of your child (and associated information) in print and online promotional, marketing, media and educational materials.

If you have more than one child at the school, and do not want to fill out a separate form for each, you can list multiple children below.

Thank you for your continued support. Please return this form to [insert].

— —

STUDENT'S NAME: _____ **YEAR LEVEL:** _____

NOTE: Please tick the boxes below to show your consent. If you do not consent, please leave the box blank.

- I give my consent to the school using/disclosing my child's personal information (including image) as described above:
  - O on the school website

- O on school social media channels available to the public (such as Facebook and Twitter)
- O in materials published by the school for the purpose of promoting the school (including school events, programs and activities)
- O in materials published by third parties (e.g., newspapers) for the purpose of promoting the school (including school events, programs and activities)

[insert any other consents you wish to seek]

- I give my consent to the [***system***]/[***CEC/[equivalent to CEC in your State or Territory]/ Diocese***] using/disclosing my child's personal information (including image) as described above:
  - O in material available free of charge to schools and education departments around Australia for the [system]/[***CEC/[equivalent to CEC in your State or Territory]/ Diocese***]'s promotional, marketing, media and educational purposes without acknowledgment, remuneration or compensation.

If you wish to **withdraw any consent** provided above, please email the school at [insert email address.]. Once consent is withdrawn, the school will not make any new publications (as applicable to the withdrawn consent - e.g., new posts to public social media pages) that include the student's personal information.

Name of Parent / Guardian _____

Signed: Parent/Guardian _____ Date: _____

If Student is aged 15+, student must also sign:
Signed: Student _____ Date: _____

ANNEXURE 8 – SHORT FORM DISCLOSURE STATEMENT TO STUDENTS

When you come to see me about an issue, it will generally be treated as confidential.

However, I need to make sure that you understand that I can't promise not to tell anyone anything that you have told me because there are some limits on the confidentiality I can provide. In other words what you tell me may need to be shared with another person or a small number of people.

The School provides student wellbeing/counselling services to help the learning and development of students at the School, and to look after their safety and welfare. I am part of those wellbeing/counselling services. That means that I can help you, but I am doing so as part of the School.

I may need to tell the Principal or their representative, or your parents, that you are coming to see me.

I will keep notes of our discussions. The Principal is able to access those notes and records as they belong to the School. The Principal may also approve someone else accessing these notes.

I may also need to share information that you have told me, if I am worried about you or think that something that you have told me could assist the School in meeting your needs.

If I need to share your information, I will share it with Principal or a senior staff member who understands the need to keep it confidential.

It is possible that the Principal or the senior staff member may need to share that information with other members of staff or may allow me to share this information with other staff, but only on a need-to-know basis.

It is also possible that the Principal or their representative will share some information I tell them with your parents.

I may also have a legal obligation to share certain information that you have told me.

Are you clear about what we have talked about?

Confirmation

I confirm that I have provided a copy of this Statement to [*insert student name*] and [*he/she*] has read the Statement.

or

I confirm that I have read the Statement to and/or explained the limits to confidentiality to [*insert student name*].

Signed _____ Dated _____

ANNEXURE 9 - SHORT FORM DISCLOSURE STATEMENT TO STUDENTS ALTERNATIVE (SAMPLE SCRIPT FOR COUNSELLORS)

The school provides student wellbeing/counselling services to assist in the learning and development of students and support safety and welfare at the school. I am part of those wellbeing/counselling services. That means that I can help you, and this is as part of my role at the school.

When you come to see me about any concerns you may have, it will generally be treated as confidential.

I may need to tell the Principal, or a senior staff member, or your parents, that you are coming to see me.

It is important that you understand that there are some limits on my confidentiality and there may be times that I need to share some information with another person or people. For example, if I am worried about you or think that something you have told me could help the school to look after you. If I need to share this with the Principal or a senior staff member, they will also understand the need to keep the information confidential and only share information with school staff on a need-to-know basis. It is also possible that the Principal, or their representative, will share some information I tell them with your parents.

I will keep notes of our discussions, and these belong to the school. The Principal, or their representative, may access these notes if they have any concerns about your safety and wellbeing.

Do you have any questions about what we talked about?

Confirmation

I confirm that I have provided a copy of this Statement to [*insert student name*] and [*he/she*] has read the Statement.

or

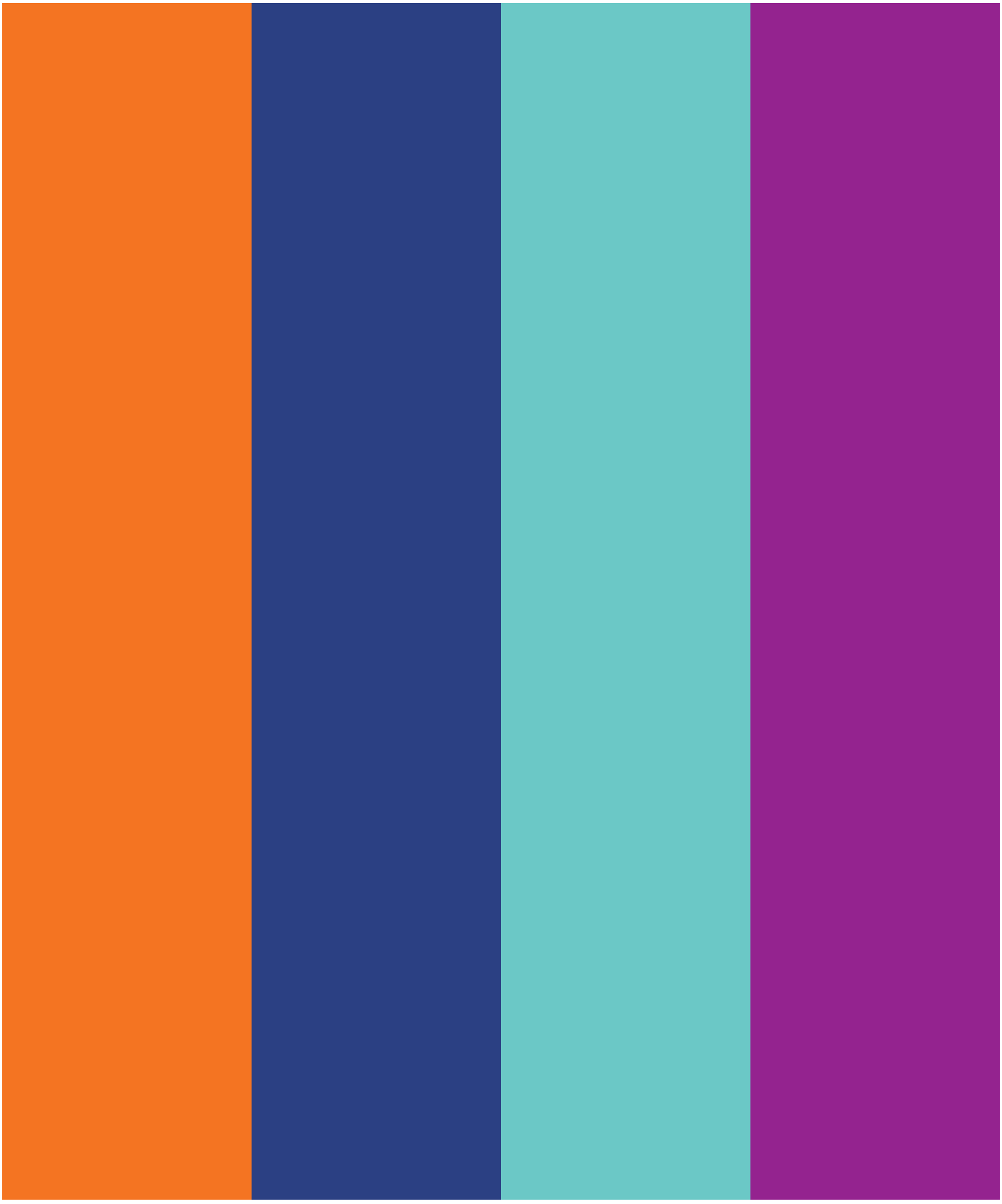
I confirm that I have read the Statement to and/or explained the limits to confidentiality to [*insert student name*].

Signed _____ Dated _____

ANNEXURE 10 – GLOSSARY OF TERMS

Term/Acronym	Definition
ABN	Australian Business Number
ACARA	Australian Curriculum, Assessment and Reporting Authority
ACORN	Australian Cyber Crime Online Reporting Network
AIS	Association of Independent Schools
ALRC	Australian Law Reform Commission
APP Entity	An organisation or other entity regulated by the *Privacy Act 1988* (Cth)
APP Guidelines	*Australian Privacy Principles Guidelines* published by the OAIC
APPs	Australian Privacy Principles contained in Schedule 1 of the Privacy Act
CEC	Catholic Education Commission
CEnet	Catholic Education Network
Centralised Systems	Centralised information management and storage systems
CERT	National Computer Emergency Response Team
CSNSW	Catholic Schools New South Wales
Data Breach	Actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure
EDB	'Eligible data breach' as defined in the Privacy Act (see Paragraph 1.4 of Part B of this Manual)
EU	European Union
FACS	Department of Family and Community Services
GAFE	Google Apps for Education
GDPR	The General Data Protection Regulation (EU) 2016/679

Term/Acronym	Definition
GRI	Government related identifier
ICSEA	Index of Community Socio-Educational Advantage
ISDTN	Interstate Student Data Transfer Note
NAPLAN	National Assessment Program – Literary and Numeracy
NDB Scheme	The notifiable data breach scheme contained in Part IIIC of the Privacy Act
NPPs	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
OAIC Resources	OAIC's *NDB Scheme: Resources for agencies and organisations* available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
Privacy Act	*Privacy Act 1988* (Cth)
PSI	Platform student identifier created for NAPALAN online.
Reasonable Belief Defence	Has the meaning given in Section 6.1(a) of Part D of this Manual.
School	Schools and systems which are represented by the National Catholic Education Commission and schools which are Members of an Association of Independent Schools.
SCSEEC	Standing Council on School Education and Early Childhood
Security Guide	*Guide to securing personal information* published by the OAIC
Student Identifier	Student identification or registration numbers issued by a Department of Education, ACARA or other State or Commonwealth authority
TFN	Tax file number
VET	Vocational Education and Training



INDEPENDENT SCHOOLS AUSTRALIA

NATIONAL CATHOLIC EDUCATION COMMISSION

ME_206281805_9