NATIONAL CATHOLIC EDUCATION COMMISSION
AND
INDEPENDENT SCHOOLS COUNCIL OF AUSTRALIA

PRIVACY COMPLIANCE MANUAL

May 2018

This Manual may be used by schools and systems which are represented by the Catholic Education Commission and by schools which are Members of an Association of Independent Schools.

FOREWORD

The Privacy Compliance Manual (updated to May 2018) supersedes the Privacy Compliance Manual which was first published in 2001 and updated in 2004, 2007, 2010, 2013, 2014, 2016, 2017 and January 2018. It contains some substantial changes which were required by the introduction of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), and also other amendments to reflect changes in other legislation and to improve the Manual generally.

In particular, it now contains a section on how to respond in the case of data breaches and eligible data breaches under the notifiable data breaches scheme. It is essential for schools to be aware there are substantial penalties for serious or repeated interferences with privacy and the Information Commissioner has the power to seek enforceable undertakings. This is quite apart from the reputational damage that a school may suffer if the privacy of an individual is breached. The notifiable data breaches scheme obligations under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) commenced on 22 February 2018.

The purpose of the Manual is to provide assistance and guidance to non-government schools corresponding with the new requirements they must observe in relation to the preservation of an individual's privacy. **A SUMMARY OF SOME OF THE REQUIREMENTS THAT SCHOOLS MUST MEET IS CONTAINED IN SECTION** 5 **AND ANNEXURE 1 OF THE MANUAL.**

The preparation of this Manual has been funded by the Associations of Independent Schools and Catholic Education Commissions in each Australian State and Territory. The previous Manual should be discarded to ensure that only the current Manual is used.

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.

TABLE OF CONTENTS

PART 1: *THE PRIVACY ACT 1988*

1. INTRODUCTION

1.1 Purpose

1.1.1 The purpose of the Manual is to assist non-government schools and systems (**Schools**) to comply with Commonwealth privacy laws.

1.2 Background - the *Privacy Act* 1988

1.2.1 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 with turnovers of over $3 million.

1.2.2 Like previous versions, this Manual sets out a guide for Schools in handling the personal information of pupils, parents, employers and other people where personal information is collected. In the Manual, the *Privacy Act* 1988 is referred to as the 'Privacy Act'.

1.3 Health Records

1.3.1 Specific legislation has been introduced in various States and Territories which imposes certain limitations on how an organisation may deal with health records.

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

1.3.3 The obligations which apply in respect of health records are set out at Section 21.

1.4 Australian Privacy Principles

1.4.1 A key component of the legislation is the mandatory requirement for a School to comply with the 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 Annexure 1.

1.5 Other Aspects of the Privacy Act

1.5.1 The Privacy Act includes mechanisms enabling individuals to:

(a) access personal information held about them;

(b) request corrections be made to that information;

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

(d) receive compensation for interferences with their privacy.

1.5.2 Schools must comply with the APPs. If a School is found to interfere with a person's privacy, the Information Commissioner can make a declaration that there has been an interference with their privacy, that compensation or damages should be paid to that person and/or that the School take steps to ensure it does not occur again. The Information Commissioner 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.

1.5.3 In addition to its obligations under law, Schools should remain alert to the Information Commissioner's powers to publicise breaches of the Privacy Act in the media.

1.6 To whom does the Privacy Act apply?

1.6.1 Under the Privacy Act, both Commonwealth agencies and private sector organisations are regulated by the APPs. The concept of an 'APP Entity' is used in the APPs to cover both types of entities.

1.6.2 There are some types of entities which will be exempt from the application of the Privacy Act. These are discussed in Paragraph 2.6.

1.7 Guidelines

1.7.1 The Information Commissioner has the power to make Guidelines about the APPs under the Privacy Act. The Guidelines are intended to provide advice and interpretation on how the APPs will operate. The Guidelines are not binding. The Commissioner has released the Guidelines for all the APPs (**APP Guidelines**). This Manual includes commentary on some of the APP Guidelines where relevant.

1.8 Important Issues

1.8.1 The Privacy Act does not differentiate between adults and children. Therefore, difficult issues arise where consents are obtained from parents for and on behalf of their children. When referring to consents and authorities throughout this Manual this should be borne in mind. The issue of consents and young people is discussed at paragraph 17.1.

1.8.2 There are some important provisions to bear in mind when dealing with records of employees. Although an 'employee record' will be exempt from the Privacy Act, Schools must be cautious when relying upon the exemption as it will only apply to an employee record held by the employing entity. Once the record is disclosed to another entity, the exemption will cease to apply in respect of that information in the hands of the new entity and the APPs will govern the handling of that information. The issue of employee records is discussed at Section 24.

1.8.3 The question of cloud computing and the location of servers is also becoming increasingly relevant to Schools who choose to outsource data storage functions to third party 'cloud' providers. The issue of cloud computing is discussed at Section 22.

1.8.4 As a result of the broad definition of 'credit provider' in the Privacy Act, many Schools will be likely to be credit providers. However, the practical effect of this is, in most cases, likely to be very small. Section 23 contains further information on the issue.

1.8.5 All schools in Australia are required to participate in the National Assessment Program – Literary and Numeracy (**NAPLAN**). NAPLAN will move online from 2018 (with some limited readiness testing occurring from 2017). Schools will be required to provide notifications to parents in relation to NAPLAN online. This is explained in Section 8.11.

2. WHAT TYPES OF INFORMATION ARE COVERED BY THE ACT?

2.1 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.

2.2 What is 'personal information'?

2.2.1 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 in a material form or not. It includes all personal information regardless of its source.

2.2.2 In other words, if the information or opinion identifies an individual or allows an individual to be identified it will be 'personal information' within the meaning of the Privacy Act. It can range from very detailed information, such as medical records, to other less obvious types of identifying information, such as an email address.

2.2.3 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 de-identified information.

2.2.4 The APPs apply to the collection of personal information by a School for inclusion in a record or a generally available publication, but apart from this, the APPs only apply to personal information a School has collected that it holds in a record.

2.3 What is 'sensitive information'?

2.3.1 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.

2.4 What is 'health information'?

2.4.1 Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. 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 21.

2.5 What is a 'record'?

2.5.1 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.

2.5.2 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.

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

(a) a generally available publication (eg. a telephone directory); and

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

2.5.4 The effect of these exclusions is discussed at Paragraphs 19.6 to 19.9.

2.6 Which acts and practices are exempt?

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

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

Small Business

2.6.3 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.

2.6.4 Although the Privacy Act defines 'health service' broadly, this exception will mainly apply to Schools that have an infirmary or a registered nurse on staff who provides health services. It possibly would include Schools that employ a psychologist to counsel students. It is likely, however, that most Schools that provide a 'health service' will have an annual turnover of greater than $3 million.

Employee records

Certain acts or practices directly relating to employee records are exempt from the scope of the Privacy Act. See Section 24 for more information on the employee records exemption.

Transfers between related companies

2.6.5 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.

2.6.6 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. 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.

2.6.7 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.

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

2.6.9 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.

2.6.10 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.

2.6.11 The related bodies corporate exemption applies only to the sharing of personal information (not sensitive information). Therefore, 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.

3. COMPLAINTS HANDLING AND APP BREACHES

3.1 Complaints handling procedure and Breach of APPs

3.1.1 The APPs require a School to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the School's functions or activities that will enable it to deal with enquiries or complaints about its compliance with the APPs.

3.1.2 Schools are also required to advise individuals in their Privacy Policy of how they may complain about a breach of the APPs and how the School will deal with that complaint. Schools are required to advise individuals in their collection statement that their Privacy Policy contains this information.

3.1.3 Complaints should be directed in the first instance to the School. The Information Commissioner may decide not to investigate a matter if the individual has not first brought a complaint to the School concerned, unless the Information Commissioner is of the view that this would be inappropriate.

3.1.4 If the complaint is unable to be resolved at the School level, the Information Commissioner may investigate the complaint. A complaint that is upheld may be resolved by an order that the entity redress any loss or damage to the person whose privacy has been breached. This could include a compensation order.

3.1.5 Notwithstanding the procedures described above, the Information Commissioner also has discretion to investigate, on his or her own initiative, an act or practice which may be an interference with privacy if the Information Commissioner thinks that it would be appropriate (eg. even where no complaint has been made by the individual involved).

3.1.6 If the entity does not comply with any orders made, the complainant can have the order enforced in the Federal Court or the Federal Circuit Court.

3.1.7 The Information Commissioner has the power to conduct an assessment of whether an entity is complying with the APPs. The Commissioner may also accept written undertakings from an entity 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 the entity does not interfere with the privacy of an individual in the future. If an undertaking is breached, the Commissioner can apply to the Federal Court or Federal Circuit Court for orders directing the entity to comply with its undertaking or to compensate anyone who has suffered loss or damage as a result of the breach of the undertaking or for any other order that the court considers appropriate.

3.1.8 Additionally, the Information Commissioner has the power to seek pecuniary penalties of up to $360,000 for individuals, and $1.8 million for entities in circumstances where there has been a serious or repeated interference with privacy.

3.1.9 The Information Commissioner has indicated that although the complaints process is designed to ensure that most complaints can be resolved through conciliation and mediation rather than through the courts, pecuniary penalties will be sought in appropriate circumstances.

4. WHAT KINDS OF INFORMATION ARE COLLECTED AND HELD BY SCHOOLS?

4.1 Personal information likely to be collected

4.1.1 The following kinds of personal information are likely to be collected and held in a 'record' (see paragraph 2.5.1).

4.1.2 For pupils 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 (eg. government welfare agencies/departments), correspondence with parents, photos, current/previous school, health fund details and Medicare number.

4.1.3 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, Medicare number, other children's details, donation history, maiden name of ex-pupils, alumni year, whether alumni had further education, professional experience and personal news.

4.1.4 For job applicants, staff members and contractors this could include:
name, company name and ABN, phone number, email address, 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, salary being sought and other salary details, details of referees, 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.

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

4.2 Sensitive information likely to be collected

4.2.1 The following kinds of sensitive information are likely to be collected and held by Schools.

(a) For pupils - religion, birth certificate, language spoken at home, religious records, whether Aboriginal, 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. Also parental education , parental occupation and other like personal/ family socio – economic information required for purposes such as, but not limited to, school funding ICSEA calculations.

(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.

4.3 Health information likely to be collected

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

(a) For pupils - 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 sensitive information contained in a doctor or hospital report.

(c) For job applicants, staff members and contractors - medical condition affecting ability to perform work, health information, compensation claims and doctor's certificates.

5. WHAT SCHOOLS NEED TO DO TO COMPLY

5.1 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:

5.1.1 Internal review:

(a) consider appointing a privacy officer or other person who will be responsible for privacy related issues; and

(b) conduct a review of current information handling practices and security procedures.

5.1.2 Analyse results of review to identify:

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

(b) why and how the School collects, uses and discloses personal information;

(c) any risk areas (eg. where there is collection and use of sensitive information or where collection, use or disclosure of personal information might not be expected by the individual); and

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

5.1.3 Privacy documentation:

(a) review and amend existing Privacy Policy or implement a Privacy Policy (this may be adapted from the draft policy in Annexure 2). The Privacy Policy must be clearly expressed and up-to-date and detail the School's management of personal information; and

(b) review any other relevant documentation (such as 'standard collection statements' and other forms) as necessary.

5.1.4 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

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

5.1.5 Continuing obligations:

(a) make the Privacy Policy available to anyone who asks for it;

(b) ensure on-going compliance (eg. regular review of information handling practices, conduct further audits where necessary, update Privacy Policy and collection notices); and

(c) ensure compliance with other applicable legislation, including health records legislation (see Section 21).

PART 2 – THE AUSTRALIAN PRIVACY PRINCIPLES

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 Annexure 1.

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

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

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

6.1.2 Requirement:
A School must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity'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 entity; 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).

6.1.3 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.

6.1.4 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. In the APPs, reference to 'steps that are reasonable in the circumstances' is to be interpreted in a similar way to 'reasonable steps' in the National Privacy Principles (**NPPs**).

6.1.5 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 a move towards a 'privacy by design' approach to compliance - that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception.

6.1.6 The significance of this principle is three-fold:

(a) this is an overarching requirement;

(b) the Information Commissioner has the power to investigate whether an entity is properly managing personal information, even where there is no breach of an APP; and

(c) if an entity 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.

6.2 How to comply:

6.2.1 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;

(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.

6.2.2 Attached at Annexure 3 are Privacy Planning Templates intended to assist a School in assessing the personal information that it currently collects and identifying risks involved.

6.3 Consent

6.3.1 Throughout the APPs there are provisions which require consent to be obtained. It is part of being open and transparent that consent is freely obtained and 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, without giving the individual the opportunity to choose which collections, uses and disclosures they consent to. The APP Guidelines provide that this practice of obtaining bundled consents has the potential to undermine the voluntary nature of the consent.

6.4 Privacy Policy (APP 1.3-1.6)

6.4.1 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).

6.4.2 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).

6.4.3 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. A School will usually make its Privacy Policy available on its website. (APP 1.5)

6.4.4 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)

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

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

6.5 How to comply:

6.5.1 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'.*

6.5.2 Draft a Privacy Policy (an example is at Annexure 2) which covers the following issues:

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

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

(c) access and correction of information;

(d) direct marketing;

(e) the transfer of information overseas;

(f) storage of information;

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

(h) complaints

6.5.3 The draft Privacy Policy at Annexure 2 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.

6.5.4 Make the Privacy Policy available on the School's website and draw attention to it when collecting personal information.

6.6 Training staff

6.6.1 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.

6.6.2 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 receipt;

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

(c) holding internal seminars and workshops.

6.7 Do's and Don'ts

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

DO encourage staff members to read the School's Privacy Policy.

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 ensure staff refer all queries about the Privacy Policy to the School's privacy officer.

7. ANONYMITY AND PSEUDONYMITY(APP 2)

7.1 Anonymity and Pseudonymity

7.1.1 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.

7.2 Comment

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

7.2.2 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.

7.3 How to comply:

7.3.1 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.

8. COLLECTION (APPS 3, 4, AND 5)

8.1 Collection

8.1.1 The APPs differentiate between 'solicited' information and 'unsolicited' information. 'Solicited information' is information that the School has asked the individual or a third party to provide.

8.1.2 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).

8.2 Sensitive Information (APP 3.3 and 3.4)

8.2.1 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 2.3.

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; and

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

8.2.2 In a large number of cases, sensitive information, including health information, will be provided by the parents or pupils 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. For example, one School may advise a second School about health issues relating to a pupil 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.

8.3 Comment

8.3.1 The Commissioner 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.

8.3.2 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.

8.4 How to comply:

8.4.1 Ensure that all items of personal information, including sensitive information, collected by the School have been identified.

8.4.2 Ensure that all items 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.

8.4.3 Ensure that sensitive information is being collected with consent or where an exception applies.

8.4.4 The Privacy Information Templates at Annexure 3 are intended to assist Schools in identifying and determining how to deal with personal information that it collects.

8.5 Lawful and fair collection (APP 3.5)

8.5.1 Requirement: A School must collect personal information:

(a) only by lawful and fair means; and

(b) not in an unreasonably intrusive way.

8.6 Comment

8.6.1 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.

8.6.2 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.

8.7 How to comply:

8.7.1 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.

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

8.7.3 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.

8.8 Ensuring the individual is fully aware of collection (APP 5.1)

8.8.1 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, 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.

8.9 Comment

8.9.1 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.

8.9.2 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 (eg, 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.

8.9.3 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.

8.9.4 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.

8.9.5 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 or billing do not have to be described.

8.9.6 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.

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

8.9.8 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.

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

8.10 How to comply:

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

8.10.2 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.

8.10.3 As the information a School requires varies over the period of a pupil's enrolment, it is suggested that the 'standard collection notice' (see Paragraph 8.12) be reviewed and updated each year.

8.10.4 However, where the School collects personal and sensitive information from those who have not seen either collection notices (eg. 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 pupil or a pupil's photo in a public forum (such as on television or on social media, such as Facebook and Flickr) the pupil's and/or the pupil's parents permission should be sought as appropriate. An example of such a permission form is contained at Annexure 5. Schools should be careful when seeking consent. To the extent that it is possible, schools should seek specific consent to use an image for a particular purpose and refrain from asking for consent where a number of uses are bundled together (see Annexure 5). In the case of the former, such consents are less likely to be acceptable under the APPs. The Annexure 5 form makes it clear that not all uses need to be agreed to.

8.10.5 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.

8.10.6 The 'standard collection notice' should be reproduced in enrolment forms and at any other initial points of collection.

8.10.7 The School should consider placing a 'standard collection notice' in other relevant documents (eg. it may be appropriate to insert a modified collection notice in a form designed to collect a pupil's medical information).

8.10.8 The 'standard collection notice' should be distributed with all enrolment forms to pupils' parents and could also be placed in each pupil's School diary. It is suggested that the then-current notice be sent at the commencement of each school year to parents of pupils at the same time as other materials are sent. A tailored employment collection form should also be used for job applicants.

8.11 NAPLAN Online Notices

8.11.1 All schools in Australia are required to participate in the National Assessment Program – Literary and Numeracy (**NAPLAN**). NAPLAN will move online from 2018 (with some limited readiness testing occurring from 2017). The privacy notifications below (as well as the draft privacy policy in Annexure 2) have been updated to reflect the personal information flows associated with NAPLAN online (including the potential disclosure by Schools of parents' and students' personal information as part of NAPLAN online).

8.11.2 Schools will also be provided with a separate NAPLAN online 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.

8.12 Standard Collection Notice

8.12.1 The following is suggested wording which seeks to achieve a combination of ensuring the individual is reasonably aware of the matters specified in APP 5.1. 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.

Sample Standard Collection Notice

1. The School collects personal information, including sensitive information about pupils and parents or guardians before and during the course of a pupil's enrolment at the School. This may be in writing or in the course of conversations. The primary purpose of collecting this information is to enable the School to provide schooling to pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the School.

2. Some of the information we collect is to satisfy the School's legal obligations, particularly to enable the School to discharge its duty of care.

3. Laws governing or relating to the operation of a school require certain information to be collected and disclosed. These include relevant Education Acts, and Public Health [and Child Protection]* laws.

4. Health information about pupils is sensitive information within the terms of the Australian Privacy Principles (**APPs**) under the *Privacy Act 1988*. We may ask you to provide medical reports about pupils from time to time.

5. The School may disclose personal and sensitive information for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools;
- government departments (including for policy and funding purposes);

- [Catholic Education Office, the Catholic Education Commission, the School's local diocese 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, [sports] coaches, volunteers, and counsellors;
- 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);
- 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.

6. Personal information collected from pupils is regularly disclosed to their parents or guardians.

7. 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. 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.**

8. The School's Privacy Policy, accessible on the School's website, sets out how parents or pupils may seek access to and correction of their personal information which the School has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others, where access may result in a breach of the School's duty of care to the pupil, or where pupils have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.

9. The School's Privacy Policy also sets out how parents and pupils can make a complaint about a breach of the APPs and how the complaint will be handled.

10. The School may engage in fundraising activities. Information received from you 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.

11. On occasions information such as academic and sporting achievements, pupil activities and similar news is published in School newsletters and magazines, on our intranet [and on our website]. this may include photographs and videos of pupil activities such as sporting events, school camps and school excursions. The School will obtain permissions [annually] from the pupil's parent or guardian (and from the student if appropriate) if we would like to include such photographs or videos [or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet. [12. We may include pupils' and pupils' parents' contact details in a class list and School directory.]†

12/13. 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.

***** As appropriate
** If applicable
† Schools may wish to seek specific consent to publish contact details in class lists and School directories

8.13 Alumni Collection Notice

8.13.1 At some Schools, pupils' personal information will be sent to the School's alumni or similar association when the pupil leaves the School. When this occurs, the School should obtain the pupil's consent and should insert an appropriate collection notice in a relevant form (eg. in an Application for membership of Alumni Association form). If the pupil 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.

8.13.2 Alternatively, the School might wish to forward to the pupil, on behalf of the Alumni Association, relevant documentation inviting the pupil to join the Association.

8.13.3 Such a collection notice could be worded as follows:

Sample Alumni Association Collection Notice

1. [The Alumni Association/We] may collect personal information about you from time to time. The primary purpose of collecting this information is to enable us to inform you about our activities and the activities of [name of School] and to keep alumni members informed about other members.

2. We must have the information referred to above to enable us to continue your membership of [the Alumni Association].

3. As you know, from time to time we engage in fundraising activities. The information received from you may be used to make an appeal to you. [It may also be used by [name of School] to assist in its fundraising activities.] [If you do not agree to this, please advise us now.]

4. [The Alumni Association/We] may publish details about you in our [name of publication] [and our/the School's website]. If you do not agree to this you must advise us now.

5. 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 has collected and holds, and how you may complain about a breach of the Australian Privacy Principles.

6. 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 also be provided to these service providers to enable them to authenticate users that access their services. 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.*

7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

* If applicable

8.14 Employment Collection Notice (for job applicants)

8.14.1 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 applying for this position you will be providing [name of School] with personal information. We can be contacted [insert address, email address, telephone number].

2. If you provide us with personal information, for example, your name and address or information contained on your resume, we will collect the information in order to assess your application for employment. We may keep this information on file if your application is unsuccessful in case another position becomes available.

3. The School's Privacy Policy, accessible on the School's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your personal information which the School has collected and holds. However, access may be refused in certain circumstances such as where access

would have an unreasonable impact on the privacy of others. Any refusal will be notified in writing with reasons if appropriate.

4. We will not disclose this information to a third party without your consent unless otherwise permitted. / We usually disclose this kind of information to the following types of organisations [insert list eg support vendors that provide services around staff administration systems].

5. [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.*] We may also collect personal information about you in accordance with these laws.*

6. 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 also be provided to these service providers to enable them to authenticate users that access their services. 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.*

7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

* If applicable

8.14.2 The employee records exemption (see Section 24) does not apply to job applicants. Therefore, under the access and correction provisions in APP 12 and 13 (see Section 15 and 16) 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 (eg. 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.

8.14.3 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 3 must still be complied with. This issue is discussed in Paragraph 8.2.

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

8.15 Contractor/Volunteer Collection Notice

8.15.1 All new contractors and volunteers should be sent a modified version of the 'employment collection notice'. This notice could be worded as follows:

Sample Contractor / Volunteer Collection Notice

1. In offering, applying or agreeing to provide services to the School, you will be providing [name of School] with personal information. We can be contacted [insert address, email address, telephone number].

2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.

3. You agree that we may store this information for [insert amount of time].

4. The School's Privacy Policy, accessible on the School's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your personal information which the School has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others. Any refusal will be notified in writing with reasons if appropriate.

5. We will not disclose this information to a third party without your consent unless otherwise permitted to. / We usually disclose this kind of information to the following types of organisations [insert list eg support vendors that provide services around administration systems].

6. [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.*] [We may also collect other personal information about you in accordance with these laws.*]

7. 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. 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.*

8. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

* If applicable

8.16 Collection through surveillance

8.16.1 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.

8.16.2 Specific legislation in certain States and Territories governs the surveillance and monitoring of persons on School grounds including pupils, 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.

8.16.3 Students, volunteers, teachers, employees and contractors should be provided with a computer usage policy. Ideally, written acknowledgement that they have received that policy should be given to the school.

8.16.4 Additionally, pupils, volunteers, teachers, employees and contractors should be notified of any other instances of surveillance in the contract of employment, through School policies or notices, or through the use of signage in areas where a School engages in surveillance.

8.17 Collection of information directly from the individual (APP 3.6)

8.17.1 Requirement:
Unless consent is obtained, if reasonable and practicable, personal information must only be collected directly from the individual.

8.18 Comment

8.18.1 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.

8.18.2 In the case of Schools this is often not practicable.

8.18.3 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).

8.19 Direct collections by Schools – Table 2A

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

8.19.1 There are also various methods of indirect collection, including interviews, forms and other documentation, telephone calls, references, and resumes.

8.19.2 The following indicates some instances of indirect collection by Schools. It is also necessary to consider the section on receipt of unsolicited personal information at Paragraph 8.31

8.20 Indirect collections by Schools – Table 2B

Individual concerned	Third party source of collection
Pupils of another school	• Principal of another school
Pupils	• Professionals (eg. counsellors, doctors, speech pathologists, therapists, other agencies) through reports and general information (eg. medical, vision, hearing, speech tests) and other results (eg. psychometric) • Parents and staff in performance appraisals
Pupils	• CEC and AIS
Pupils	• School (teachers, principal, boarding master) (eg. where computer use is monitored, certain access to personal and disciplinary information)
Pupils	• Parent through various forms (eg. enrolment form, medical advice form, deed of indemnity)
Pupils	• Government welfare agencies/departments (regarding safety of child at home)
Pupils	• Parent (and vice versa)
Pupils and staff members	• Pupils and/or staff members through various forms (eg. incident report, Child Protection Notification Form)
Pupils, staff members, others	• Pupils who name them to counsellors or staff members during counselling or advising or in an incident report
Pupils and parents	• Priests (reference) • Previous school (reference)
Pupils or prospective pupils in New South Wales	• Another school for the purpose of assessing whether the enrolment of the pupil or prospective pupil 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 (eg. P&F, development office for fundraising) • Medical practitioners (eg. mother has cancer) • School (eg. in Pupil Report Card)
Pupils' family members	• Pupil (eg. pray for sick parent or Grandparent)

* Please refer to Paragraph 19.5 for more information.

8.20.1 The following indicates some further instances of indirect collection by Schools.

8.21 Further indirect collections by Schools - Table 2C

Individual concerned	Third party source of collection
Employees and Contractors	• Referees who provide information upon request
Previous employers	• Staff members and job applicants through various forms (eg. application form) and resume

Individual concerned	Third party source of collection
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	• Pupils, staff members and parents through various forms (eg. enrolment form)
Emergency contacts	• Pupils, staff members and parents through various forms (eg. enrolment form, staff detail form)
Nominated siblings/family members	• Pupils and parents through various forms (eg. enrolment form)
Doctor	• Parent (eg. from enrolment form, pupil information sheet)
Others	• photographs

8.21.1 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 consent can be inferred. However, this may not always be the case.

8.21.2 Where a job applicant is aware that a referee is providing information about them to a School (therefore indirect collection), it can be implied that they consent to that indirect collection. However, if the School collects personal information from a referee or third party without the applicant's knowledge (eg. the job applicant's current employer), the School should advise the individual that they have collected the information. Schools should note however that 'collection' only relates to information that is contained in a record. Information obtained from a inquiry which is not recorded does not constitute a record and therefore no collection occurs.

8.22 How to comply:

8.22.1 There may be some circumstances in which information should only be collected directly from the individual. These circumstances should be considered on a case by case basis.

> Example:
> Where it is likely that the information is incorrect (eg. 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.

8.23 Collection, use and disclosure with third parties and contractors (APP 3.6 and APP 6)

8.23.1 Where the School engages a contractor or third party the following may occur:

(a) the School collects personal information from a contractor or third party;

(b) the School discloses personal information to a contractor or third party; or

(c) a contractor uses or discloses personal information on behalf of the School.

8.24 How to comply:

8.24.1 To facilitate compliance with the APPs the School should specifically require their contractor in a written agreement to keep personal information they are provided about parents and pupils confidential and only use it for the purposes of the School. The implications under the Privacy Act where the School deals with contractors is discussed further in Section 20.

8.25 Collecting sensitive information with consent

8.25.1 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.

8.26 Collecting sensitive information without consent

8.26.1 In most situations Schools will collect sensitive information with consent on the basis that it has been provided to them directly by the pupil, the parent or a person authorised by the parent such as a doctor.

8.26.2 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 the person or to public health or safety. If, for example, the child is very young he or she may be incapable of giving informed consent. It may also 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.

8.27 How to comply:

8.27.1 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 are in Paragraph 17.1. Consent, where needed, may be able to be given by the parent.

8.27.2 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.

8.27.3 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 (eg. job applicant, pupil or parent) is made aware that their sensitive information is likely to be collected, and to obtain their consent to such collection. To achieve this, a sensitive information collection notice is included in the 'standard collection notice'. It may be appropriate on some occasions to get specific consent and give a specific collection notice.

8.27.4 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 information requested in enrolment and various medical forms (eg. as required under the public health legislation); and
>
> (b) certain criminal record checks (eg. as required under child protection laws in some States).

8.27.5 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.

8.27.6 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.

8.27.7 Information about religion, racial and ethnic origin (also sensitive information) is in a different category. If this information is collected from the individual or a parent 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.

8.27.8 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:

> 'The child who is the subject of this information or the child's parent/guardian has consented to its collection by the School.'

8.27.9 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 8.26.

8.27.10 Tables 3A, 3B and 4 below illustrate the steps to be followed by the School in deciding whether it can collect personal and sensitive information.

8.28 Personal Information (Excluding Sensitive Information) Collection Table 3A

Collection	Provider	Consent	Collection Notice
Personal information about Pupil	Pupil	Not required	Covered by 'standard collection notice' to parent

Collection	Provider	Consent	Collection Notice
	Parent	Not required	Covered by 'standard collection notice' to parent
	Third party (eg. principal of another School)	Not required	Covered by 'standard collection notice', **or**, a 'special collection notice'*
Personal information about parent	Parent	Not required	Covered by 'standard collection notice' to parent
	Pupil	Not required	Covered by 'standard collection notice', **or**, a 'special collection notice', **or** failure to notify because of duty of care to pupil
	Third party (eg. another parent)	Not required	Covered by 'standard collection notice', **or**, a 'special collection notice'
Personal information about Employee ****	Employee or Third party	N/A - Employee Exemption	N/A - Employee Exemption
Personal information about Contractor / Third party	Contractor / Third party	Not required	Should be given unless obvious

* **Note:** In New South Wales, collection of personal information about pupils and prospective pupils 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 pupil would pose a risk (because of the behaviour of the pupil) to the health or safety of any person (including the pupil); and

(b) to develop and maintain strategies to eliminate or minimise that risk.

See "A Guide for NSW Non-Government Schools on Reporting, Disclosing and Exchanging Personal Information for the Purposes of Child Wellbeing".

**** 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.*

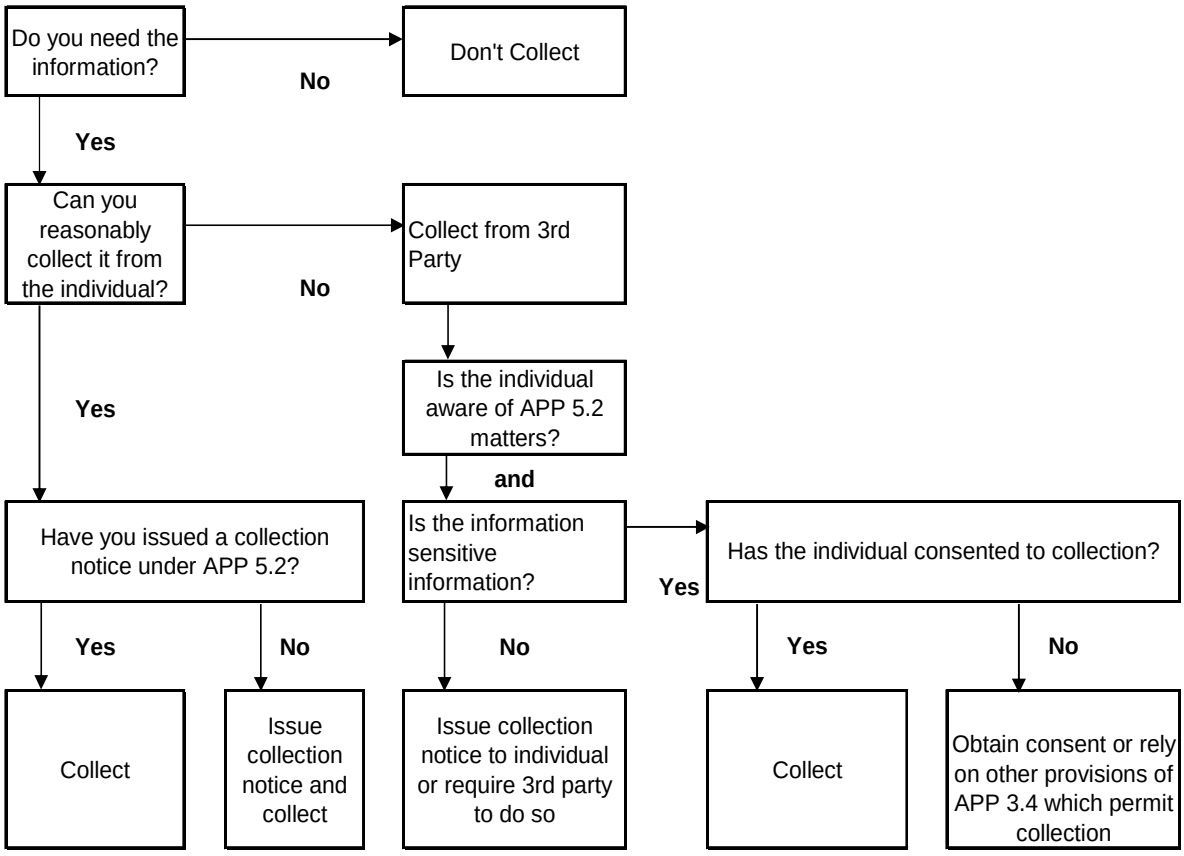
8.29 Sensitive Information Collection Table 3B

Collection	Provider	Consent	Collection Notice
Sensitive information about Pupil	Pupil	Parent to consent on behalf of Pupil	Covered by 'standard collection notice' to parent
	Parent	Parent to consent on behalf of Pupil	Covered by 'standard collection notice' to parent
	Third party (eg. doctor, principal of another School)	Parent to consent on behalf of Pupil	Covered by 'standard collection notice', **or**, a 'special collection notice'

Collection	Provider	Consent	Collection Notice
Sensitive information about parent	Parent	Consent implied	Covered by 'standard collection notice' to parent
	Pupil	Consent could be implied in some circumstances, but not always	Covered by 'standard collection notice', **or**, a 'special collection notice', **or** failure to notify because of duty of care to pupil
	Third party (eg. another parent)	Consent could be implied (eg. in case of illness), but not always	Covered by 'standard collection notice', **or**, a 'special collection notice'
Sensitive information about Employee *****	Employee or Third party	N/A - Employee Exemption	N/A - Employee Exemption
Sensitive information about Contractor / Third party	Contractor / Third party	Consent implied	Should be given unless obvious

*** Note:** See the provisions relating to health information at Section 21. In Victoria and the Australian Capital Territory, there is no exemption for a school which collects health information about its employees and, accordingly, consent must be obtained.

8.30 Collection Compliance Steps - Table 4



8.31 Unsolicited Personal Information (APP 4)

8.31.1 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.

8.31.2 This is a new provision which 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 8.2.

8.31.3 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 pupil 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.

Example:
A parent advises the School that a pupil 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 pupil. In the circumstances, it is also reasonable to take no steps to inform the mother or pupil of the collection of the information.

8.32 Do's and Don'ts

DO only collect personal information that the School requires to carry out its functions and activities.

DO identify the School and its contact details when collecting personal information.

DO inform individuals that they can access their personal information, subject to the requirements of the Privacy Act.

DO inform individuals of any plans to disclose their personal information to others.

DO consider, and notify individuals of, all the reasons for which you are collecting their personal information.

DO take reasonable steps 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 individual does not disclose 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 (eg. next of kin details) unless it is unreasonable or impracticable for you to contact the individual directly.

DON'T collect unsolicited information if it is not reasonably necessary for a function or activity of the School.

8.33 Additional Do's and Don'ts for sensitive information

DO only use sensitive information for the purposes for which it was disclosed.

DO obtain consent if you collect sensitive information unless an exception applies.

DON'T collect sensitive information unless it is necessary.

9. USE OR DISCLOSURE OF PERSONAL INFORMATION (APP 6)

9.1 Use and Disclosure

9.1.1 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 prevent serious threats to life, health or public 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 engaged in and 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)).

9.2 Primary and related purpose

9.2.1 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 pupil or receive a service. This is the 'primary' purpose of collection, even if the entity has some additional purposes in mind.

9.2.2 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.

9.2.3 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.

9.2.4 *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.

9.2.5 *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'.

9.2.6 *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).

9.2.7 *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.

9.2.8 In many instances of collection a separate consent can be obtained, resulting in the information being used or disclosed with consent. Also, information may be used or disclosed from two different sources of personal information.

9.3 Use and disclosure of information about pupils – Table 5A

9.3.1 Personal information is used and disclosed by Schools about pupils 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.

Category	Use & Disclosure of personal and sensitive information about Pupils
Primary purpose	*Personal information and sensitive information* • broadly to provide its educational services (but the precise purpose will depend on the circumstances)
Secondary purpose (related and reasonably expected)	*Personal information* • send newsletters, magazines, mail-outs and correspondence • to include in newsletters, magazines and mail-outs • administration (eg. records of attendance) • provide reports to parents

Category	Use & Disclosure of personal and sensitive information about Pupils
Secondary purpose (directly related and reasonably expected)	*Sensitive information* • compliance with law (eg. 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 (eg. administering medication) • compiling health record lists and medication lists • doctor or hospital (for medical assistance)

9.4 Use and disclosure of information about parents – Table 5B

9.4.1 Personal information about parents is used 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.

Category	Use & Disclosure of personal and sensitive information about parents
Primary purpose	*Personal information and sensitive information* • broadly to provide educational services to pupils (the precise purpose will depend on the circumstances)
Secondary purpose (related and reasonably expected)	*Personal information* • send newsletters, magazines, mail-outs and correspondence • for committees
Secondary purpose (directly related and reasonably expected)	*Sensitive information* • compliance with law (eg. a law relating to child protection - where a parent volunteers to drive a car for an excursion)
Direct Marketing	• fundraising • marketing for potential enrolments

9.4.2 Personal information about contractors is used 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.

9.5 Use and disclosure of information about contractors – Table 5C

Category	Use & Disclosure of personal and sensitive information about contractors
Primary purpose	*Personal information and sensitive information* • to engage the contractor
Secondary purpose (related and reasonably expected)	*Personal information* • to pay invoice

Secondary purpose (directly related and reasonably expected)	*Sensitive information* • To manage workers' compensation claim

9.6 How to comply:

9.6.1 A 'standard collection notice' should help overcome the potential for confusion as for what purposes the information can be used and any resultant possible breach of APP 6.

9.6.2 Schools need to consider their enrolment and employment forms through which personal information is collected to ensure that they include a collection notice (see paragraphs 8.12 and 8.14).

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

9.7.1 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.

9.7.2 Disclosure authorised by law in New South Wales

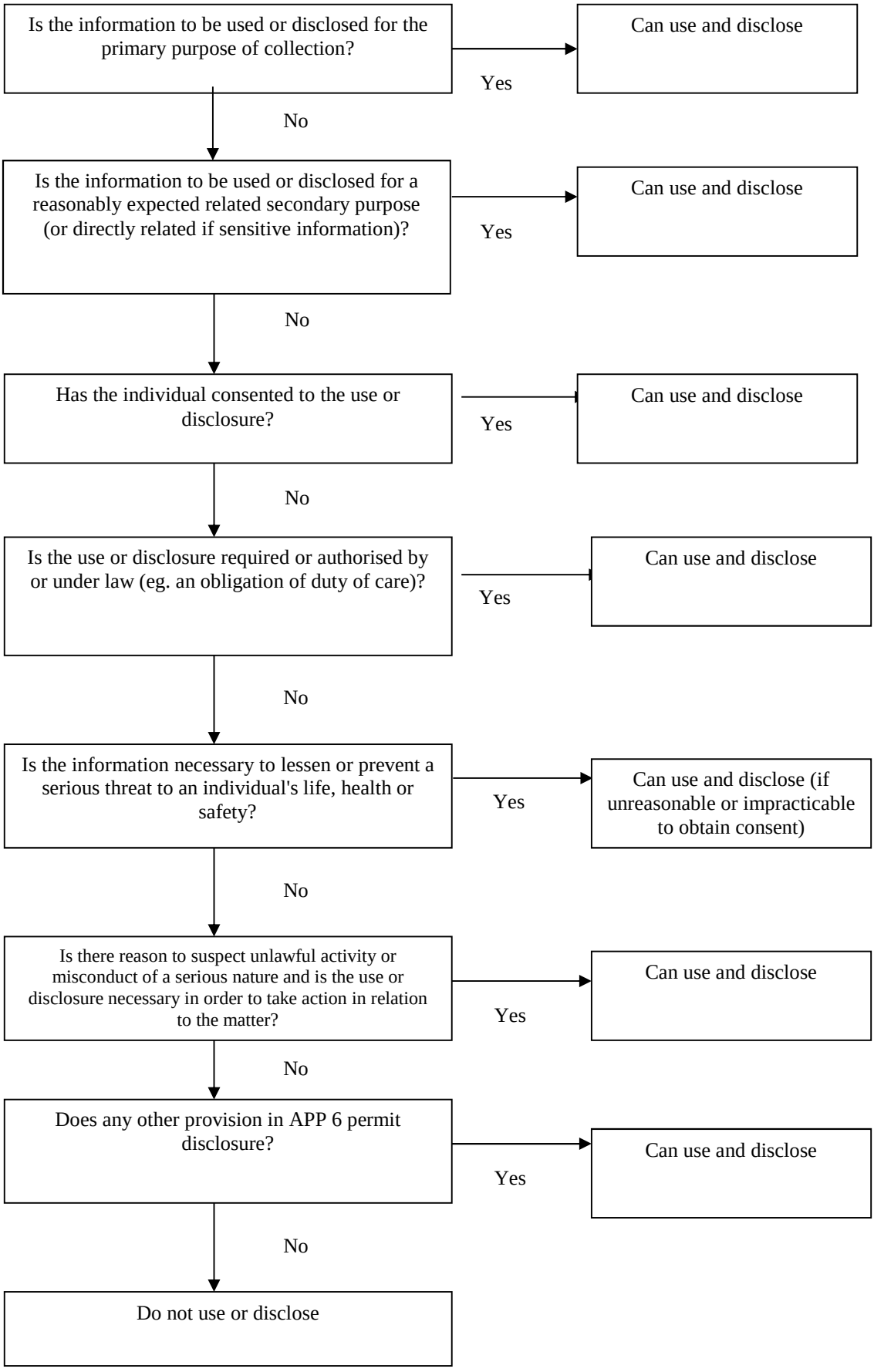
In New South Wales, specific legislation authorises disclosure of personal information relating to a pupil, prospective pupil, staff volunteers and parents for certain child protection purposes. For detailed information see 'A Guide for NSW Non-Government Schools on Reporting, Disclosing and Exchanging Personal Information for the Purposes of Child Wellbeing'.

9.8 How to comply:

9.8.1 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.

9.8.2 Table 6 illustrates what steps should be taken by the School in deciding whether it can use or disclose personal and sensitive information.

9.9 Use & Disclosure Compliance Steps - Table 6



9.10 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.

10. DIRECT MARKETING (APP 7)

10.1 Direct Marketing

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 entity 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).

10.2 Comment

10.2.1 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 or SMS. A campaign to boost enrolments is an example of a direct marketing campaign by a School.

10.2.2 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.

10.2.3 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.

10.2.4 A School may use non-sensitive personal information for direct marketing where, among other things, 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.

10.2.5 *'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 the collection notice;

(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.

10.3 How to comply:

10.3.1 Individuals that have been provided with the 'standard collection notice' (or are otherwise aware of its contents) should reasonably expect their personal information to be used for particular related secondary purposes. However, if direct marketing communications are to be sent to people who have not been provided with the 'standard collection notice' or are not otherwise aware of its contents, then the School may need to rely on APP 7.3 to send the direct marketing communications. If so, 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 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.

10.3.2 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.

10.3.3 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.

10.3.4 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. In that case, the organisation should assess whether it is impracticable to obtain consent at the time of the proposed use or disclosure.

11. CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION (APP 8)

11.1 Cross-border Disclosure

11.1.1 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. 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 entity 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; or

(c) the disclosure is required or authorised by law.

11.2 How to comply:

11.2.1 APP 8 is a new provision which places greater obligations on entities than were required under the transborder data flow provision in the NPPs. If a School relies on having taken 'reasonable steps' or an exception does not apply, and a data breach occurs the School may be liable for any breach of privacy by the overseas entity in relation to the disclosure of the School's record.

11.2.2 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 are located overseas; 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 are located overseas.

11.2.3 Online or 'cloud' service providers (referred to in paragraphs 11.2.2(c) and (d) above) use servers that may be located outside Australia, sometimes in multiple or changing locations. If the server 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.

11.2.4 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.

11.2.5 If a School is using an offshore cloud service for **more** than storing and ensuring the School may access the personal information, the School will also be required to advise people in collection notices that their personal information may be disclosed or sent offshore and, if known, to which countries. 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.

11.2.6 Compliance with APP 8 can be achieved if 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 there will remain local liability of schools for breaches of the APPs by overseas recipients); 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).

11.2.7 It is strongly suggested that if a School enters into a contract with a recipient of personal information such as a 'cloud' provider, 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. More detailed comments about cloud computing are contained at Section 22.

11.2.8 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 pupils, 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 continued access to any personal information on its system on behalf of the School 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;

(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.

11.2.9 If a School needs to disclose personal information for a particular purpose in specific circumstances (eg, 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 [***eg. facilitating a student exchange***].
>
> * I/We acknowledge that we are aware that the overseas recipient may not be bound by laws which provide the same level of protection for personal information provided by the Australian Privacy Principles and agree the School will not be responsible for any breach of privacy by [***the recipient or class of recipients***].
>
> *If applicable

11.2.10 A number of pupils attending various Schools are full fee paying overseas pupils (ie. the pupils' parents are located overseas). It can be reasonably assumed that the sending of personal information about the pupil to the parents will not cause an issue. If however the parents or pupil require personal information to be sent to a third party overseas an express consent should be obtained.

11.3 Do's and Don'ts:

> **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 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.

12. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS (APP 9)

12.1 Identifiers

12.1.1 Requirement:
APP 9 requires that identification devices provided by a government agency, such as a Medicare number, a Social Security 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 identification of the individual or to fulfil its obligations to an agency or State or Territory authority.

12.2 Comment

12.2.1 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 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.

12.2.2 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.

12.2.3 For these reasons, specific tax file number (**TFN**) legislation already restricts the way an organisation can collect, use or disclose a TFN.

12.2.4 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 8 of this Manual).

12.2.5 APP 9 does not apply to an individual's name.

12.3 How to comply:

12.3.1 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 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.

12.3.2 Additionally, when using or disclosing GRIs, the School must ensure that such use or disclosure is permitted by APP 9 (eg. 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).

12.3.3 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.

12.4 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.

13. DATA QUALITY (APP 10)

13.1 Data Quality

13.1.1 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.

13.1.2 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.

13.2 Comment

13.2.1 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.

13.2.2 The APPs require 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.

13.2.3 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. 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.

13.3 How to comply:

13.3.1 The School should establish standard procedures to ensure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

13.3.2 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.

13.3.3 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.

13.3.4 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.

13.4 Sharing personal information

13.4.1 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 to/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 2.6 regarding the related companies exemption.

13.4.2 What procedures are put in place in this regard will likely depend upon the size of the School.

13.5 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 (eg. 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 (eg. health information) and take appropriate steps.

DO investigate any clear inconsistencies with personal information held (eg. recorded as a male, but is an ex-pupil 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 purpose of the disclosure, if this is not clear.

DON'T continue to use information you believe to be out of date or inaccurate.

14. DATA SECURITY (APP 11)

14.1 Security of Personal Information

14.1.1	Requirement: A School must take reasonable steps to protect personal information it holds from misuse, interference and loss, and unauthorised access, modification or disclosure.

14.1.2 As previously noted, Schools collect large amounts of personal information ranging from names and addresses to health information 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.

14.1.3 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 financial information and sensitive information (particularly health information) will be afforded a high level of protection.

14.1.4 The requirement that reasonable steps must be taken to prevent 'interference' with personal information is intended to cover the unlawful accessing of electronic databases.

14.1.5 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.

14.1.6 Information on cloud computing is contained at Section 22.

14.1.7 The Office of the Australian Information Commissioner issued a Guide to securing personal information (the 'Security Guide') in January 2015, which can be accessed at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

14.2 Typical areas of concern

14.2.1 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

- Are there policies in place to restrict access which are administered by a dedicated staff member?
- 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?

14.3 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:

(a) the nature of the entity holding the personal information;

(b) the amount and sensitivity of personal information held;

(c) the possible adverse consequences for an individual in the case of a breach;

(d) the practical implications of implementing the security measure, including time and cost involved; and

(e) whether a security measure is in itself privacy invasive,

In determining 'reasonable steps', regard should be given to the matters set out in 14.2 and 14.3 above.

14.4 How to comply:

14.4.1 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.

14.4.2 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 unauthorised access to that information is minimised.

14.4.3 If some personal information about pupils 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 a number of parents and pupils had access to an area which contained some children's names and their medication requirements, 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. A common sense approach should prevail.

14.4.4 Staff members taking records of personal information outside School grounds (eg. 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.

14.4.5 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.

14.4.6 The need for policies and security measures in respect of computer, email and Internet use should be reviewed.

14.4.7 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.

14.4.8 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.

14.4.9 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.

14.5 Use of the Internet and emails

14.5.1 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.

14.5.2 Reasonable steps must be taken so that email communications, and the personal information contained therein, are secure in order to prevent unauthorised access. Emails and website collection points will require the use of appropriate collection notices, and in the case of emails that are direct marketing communications, contain opt-out statements and mechanisms (as well as be sent with consent).

14.6 Destruction and permanent de-identification (APP 11.2)

14.6.1 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.

14.7 Comment

14.7.1 A School should have in place systems for destroying or de-identifying personal information that is no longer needed.

14.7.2 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.

14.7.3 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.

14.7.4 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.

14.7.5 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.

14.7.6 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'.

14.8 How to comply:

14.8.1 Personal information which is no longer required for an authorised purpose should be destroyed or permanently de-identified.

14.8.2 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; and

(c) whether destroying the information would likely have a prejudicial effect on the School's operations.

14.8.3 Schools may also wish to discuss with their insurer and/or legal adviser what records should be kept and for how long.

14.8.4 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.

14.8.5 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.

14.8.6 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.

14.8.7 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 (eg. 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.

14.9 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 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 (ie. 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 cases 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 specially secure. For example, if staff leave their computers for an extended period of time, it should be shut down or they should log off or use a screensaver with password. Don't leave files where they may be accessed by unauthorised people.

DON'T ever allow unauthorised access, modification or disclosure of personal information.

15. ACCESS (APP 12)

15.1 Access to Personal Information

15.1.1 A School must on request provide the individual with access to his or her own personal information.

15.1.2 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)).

15.1.3 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).

15.1.4 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).

15.1.5 Where access is denied, the School may consider whether the use of mutually agreed intermediaries would allow sufficient access (APP 12.6).

15.1.6 The School must not charge excessive fees for providing access (APP 12.8).

15.1.7 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).

15.2 Comment

The APP Guidelines provide that access can be achieved by:

(a) providing the individual with a copy of the information;

(b) deleting any personal information for which there is a ground for refusing access and giving the redacted version to the individual;

(c) giving a summary of the requested personal information to the individual;

(d) giving access to the requested personal information in an alternative format;

(e) facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes;

(f) facilitating access to the requested personal information through a mutually agreed intermediary.

15.2.2 *Unreasonable impact on the privacy of others*

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.

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 from which the identity of the person could be reasonably ascertained.

> Example:
> Student A's parents ask for records from a School in relation to an investigation of a fight between pupils where a pupil was injured. The records disclose the name of various pupils who have given statements implicating Student A as having started the fight and causing the injuries. Providing access to records which identified the pupils who provided those statements would be likely to have an unreasonable impact upon them.

15.2.3 *Frivolous or vexatious requests*

Frivolous and vexatious requests could include those that are:

(a) trivial and made for amusement's sake;

(b) made as a means of pursuing some unrelated grievance against the organisation; or

(c) repeated requests for access to the same personal information.

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

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 18. 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.

15.3 How to comply:

15.3.1 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.

15.3.2 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.

15.3.3 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.

15.3.4 APP 12 only gives individuals the right to access personal information which the School holds about that individual. 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.

15.3.5 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 Pupil Form' in relation to an incident is not to be made available to 'other' pupils. This could possibly include pupils who are the subject of the incident and report (eg. in the case of bullying).

15.3.6 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 (eg. 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.

15.3.7 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. This is intended to ensure that entities work with individuals to try to satisfy their request. It may be that the use of a mutually agreed intermediary may permit sufficient access.

> Example:
> An example of using an intermediary is where access is requested to a pupil's file which includes personal information of other pupils 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.

15.3.8 *Time periods*

A School must respond to access 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.

15.4 Particular Issues

15.4.1 Various issues might arise where a pupil seeks access to their personal information contained in records held by the School. Where a record of personal information about a pupil contains information which would normally not be released, the School would need to consider whether it may refuse or restrict access under APP 12.

15.4.2 Examples of scenarios where a School might consider restricting access may include where the information is contained in:

(a) a psychiatric report (eg. pupil exhibits anti-social behaviour);

(b) a psychometric test (eg. indicating that the pupil has the mental capacity of a 9 year old when the pupil is 15 years old);

(c) a confidential communication between the School and a parent about their child who is a pupil of the School; and

(d) Scholarship exam results, internal marks, teachers' notes.

15.4.3 Where access to the information may adversely impact on the pupil, 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.

15.4.4 If a parent of the pupil seeking access does not consent to their child having access, this should also be considered.

15.5 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 access their information. This must 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.

16. CORRECTION

16.1 Correction of Personal Information (APP 13)

16.1.1 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 entity 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).

16.1.2 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).

16.1.3 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).

16.1.4 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).

16.1.5 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).

16.2 Comment

16.2.1 *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 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.

16.2.2 *'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.

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.

16.2.3 *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.

16.2.4 *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.

16.3 How to comply:

16.3.1 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.

16.3.2 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.

16.3.3 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.

16.3.4 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.

16.4 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 must 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 3 SPECIAL ISSUES FOR SCHOOLS

17. CONSENT AND YOUNG PEOPLE

17.1 Consent and Young People

17.1.1 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 pupils.

17.1.2 In relation to consent and young people, the APP Guidelines provide as follows:

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

17.1.3 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.

17.1.4 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.

17.1.5 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 duties at law.

17.1.6 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.

17.1.7 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.

17.1.8 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 pupils or from parents is likely to follow current practices. Thus, for example, where a pupil puts his or her name down to take part in a team, the pupil would usually be impliedly consenting to it being disclosed to a relevant party to enable him or her to compete. As a pupil reaches greater maturity, the more important it will become to consider whether a parent should be asked for consent or the pupil. Hopefully in most cases common sense will provide the answer.

17.1.9 For example, in most cases it would be appropriate for the School to collect from a mature pupil personal (and sensitive) information about the pupil gained through an interview with the pupil. Also, there will be many instances throughout a pupil's schooling where it would be impracticable and inappropriate to first obtain a parent's consent when collecting personal information from a pupil (eg. during day to day classroom activities). In respect of collecting personal information about pupils 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, then pupils do not have to be specifically informed.

17.1.10 Another potential concern is that pupils may attempt to claim a right to prevent disclosure of personal information to a parent, such as their School report. The 'standard collection notice' seeks to overcome this by informing parents that the School will disclose personal information about a pupil to the pupil's parents. If a pupil attempted to restrict disclosure of personal information (such as a School report) to a parent, it is reasonably clear that this would be a permitted purpose as being a related purpose to the purpose for which the information was collected. This does not prevent the School exercising its discretion to restrict disclosure of the personal information.

17.1.11 See Section 15 in relation to pupils seeking access (under APP 12) to their personal information which is contained in records held by the School.

17.1.12 Particular issues may arise in the context of information provided to staff members, including counsellors, by pupils 'in confidence' that is, where the pupil has asked or expected the staff member not to disclose it. This is discussed more fully at Section 18. However, one factor when considering how to deal with such situations will be the age and capacity of the pupils to provide or refuse consent.

18. DUTY OF CARE AND OBLIGATIONS OF CONFIDENCE

18.1 Duty of Care, Obligations of Confidence and the APPs

18.1.1 As discussed in Section 8 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.

18.1.2 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 pupils 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 pupils and possibly others (eg. 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 in charge of a pupil that the pupil suffers from a particular health problem.

18.1.3 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.

18.1.4 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. That said, it would be useful for Schools to make it clear in, for example, a collection notice or Privacy Policy that there may be occasions where confidences cannot be maintained.

18.1.5 Another issue to keep in mind is that 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.

18.1.6 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.

18.1.7 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 pupil 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 pupil. This is not because it was confidential so much as because of the School's duty of care to the pupil. It may also have an unreasonable impact on the privacy of the pupil (APP 12.3(b)).

19. PERSONAL INFORMATION AND THE SCHOOL COMMUNITY

19.1 Passing Information in a School Community

19.1.1 Schools like to see themselves as 'communities'. The School community will typically consist of staff, pupils, parents, past pupils 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.

19.1.2 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 (which would constitute a 'record' when filed) to a priest that a child or child's parent is sick would not be unusual. Technically this could not be done without the consent of the parent. However, if the Principal is confident consent would be given, or indeed his passing on the information would be expected, then failure to adhere to the 'letter of the law' would be unlikely to have any repercussions.

19.1.3 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, provided it was contained in a record, but is unlikely to cause offence. However, on occasions it may, particularly if the individual wished their illness to be confidential, therefore caution should be exercised in this regard.

19.1.4 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 a reasonably expected related (or directly related) purpose of obtaining the information.

19.1.5 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.

19.2 Religious Information

19.2.1 Where religious information about an existing or potential pupil or parent is sought from a priest or minister, it would be wise to obtain consent. This can be achieved in appropriate applications or enrolment forms.

19.3 Fundraising

19.3.1 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 'standard collection notice' in Paragraph 8.12.

19.4 Passing personal information to other Schools

19.4.1 Where another School which is not within the same system or is not a related corporation requests personal information about a pupil 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.

19.4.2 From 1 January 2006, 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 pupil 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 pupil.

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

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

19.4.5 The consent regime is as follows:

(a) where the information is to be passed from one non-government school to another, parent or pupil consent is **not required** before the information can be passed if the previous school has a data collection notice which conforms to the notice at Paragraph 8.12 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.

19.4.6 Information about the ISDTN and Protocol and the relevant consent forms can be found at the website of the Standing Council on School Education and Early Childhood (**SCSEEC**) at http://www.scseec.edu.au/Publications/ISDTN.aspx.

19.5 Disclosure of information where required by legislation

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

(a) *Children and Young Persons (Care and Protection) Act* 1998;

(b) *Education Amendment (School Attendance) Act* 2009;

(c) *Ombudsman Act* 1974;

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

(e) *Commission for Children and Young People Act* 1998.

A summary of the relevant provisions of these Acts is contained in "A Guide for NSW Non-Government Schools on Reporting, Disclosing and Exchanging Personal Information for the Purposes of Child Wellbeing".

19.5.2 Similar provisions may also be found in the following legislation:

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

(b) Queensland: *Child Protection Act* 1999, *Child Protection Regulation* 2011, *Commission for Children and Young People and Child Guardian Act* 2000, and *Education Act* 2006; and

(c) 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.

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

19.6 School Directories

19.6.1 The use and disclosure of school directories and class lists which contain pupils' and parents' name and contact numbers and similar information 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 Paragraph 8.12). Experience has shown that some parents do not want their details to be included on class lists.

19.7 Personal information not in a 'record'

19.7.1 The APPs apply to personal information collected for inclusion in a 'record' (eg. through an enrolment form). What is meant by 'record' is discussed at Paragraph 2.5. Under the Privacy Act a 'record' does not include many things, including:

(a) a generally available publication; and

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

19.8 School Publications

19.8.1 School publications, such as newsletters, magazines and alumni publications usually contain personal information obtained either from the relevant individual or from other sources.

19.8.2 Where a School intends to include personal information about an individual in a school publication, the individual should be made aware of this before the information is published. This could be achieved, for example, through clear wording in a collection notice provided to the individual at the time the personal information is collected (see Section 8) .

19.8.3 Sensitive information (such as health information) should not be included in school publications without consent.

19.9 Library Collections

19.9.1 The Privacy Act excludes 'anything kept in a library' from the definition of 'record'. Thus the APPs do not apply to material contained in library collections.

19.10 Systems and Schools Conducted by Church Bodies

19.10.1 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'.

19.10.2 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.

19.10.3 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.

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

19.10.5 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. However, where employment information is transferred to another entity, the employee exemption will not apply to that record in the hands of that other entity.

19.10.6 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.

19.10.7 When a School is not related to a second School it cannot rely upon section 13B of the Privacy Act 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.

20. PRIVACY IMPLICATIONS FOR SCHOOLS DEALING WITH CONTRACTORS

20.1 Privacy Implications for Schools Dealing with Contractors

20.1.1 The following information is based on, and adapted from, Information Sheet 8 released by the office of the Federal Information Commissioner in relation to equivalent provisions under the Privacy Act and the NPPs.

20.2 Contractors

20.2.1 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.

20.2.2 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.

20.2.3 The following information covers situations where the School and the contractor would be regarded under the Privacy Act as separate entities.

20.2.4 In practical terms there may be little difference in these two situations in what the School needs to do to meet its obligations.

20.3 Contracting with businesses not covered by the Privacy Act

20.3.1 An important consideration for a School entering into a contract described above will be whether the Privacy Act covers the contractor. For example, the contractor may be a small business and be exempt from having to comply with the APPs. See Paragraph 2.6.

20.4 Disclosure to Contractors

20.4.1 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 may need to 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.

20.4.2 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.

20.5 The Contracting Organisation (School)

20.5.1 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' 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'.

20.5.2 What other details about the contractor and relevant to APP 5.2 the School makes an individual aware of 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.

20.6 The Contractor

20.6.1 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.

20.6.2 In some cases it could be reasonable for no steps to be taken under APP 5.1. An example of this could be where all of the following apply:

(a) the provisions of the contract have very strong and comprehensive privacy provisions that place stringent obligations on the contractor;

(b) where the School is prepared to monitor the contractor to ensure that it complies with the APPs; and

(c) the School is prepared to take ultimate responsibility for any breach of privacy the contractor commits (although it could still seek indemnities from the contractor).

20.7 Collecting Sensitive Information Under a Contract

20.7.1 A contractor that collects sensitive information would need to have the individual's consent.

20.8 APP 6: Use and Disclosure of Personal Information

20.8.1 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 (eg. mailing activities).

20.8.2 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).

20.8.3 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 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 (see Paragraph 8.23).

20.9 APP 11: Security of Personal Information

20.9.1 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).

20.9.2 A contractor that is not a small business and which collects personal information from the School would have obligations of its own under APP 11 to keep the information secure.

20.10 Notifying Data Breaches

20.10.1 The contract should make clear that the contractor must notify the School if there is a Data Breach that affects personal information it holds and provide assistance to the School in responding to any Data Breach (including in relation to gathering the information required for notification to the Information Commissioner and individuals if there is an eligible data breach (**EDB**)).

20.10.2 The contract should also make clear who is to notify the Information Commissioner and individuals if there is an EDB under the notifiable data breaches scheme (**NDB Scheme**) (see Section 26).

21. HEALTH INFORMATION

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 pupils and staff and on occasions parents. They need to take particular care in collecting, using and disclosing health information.

21.2 What is Health Information?

21.2.1 Under the Privacy Act '*health information*' includes information or an opinion about:

(a) the health or disability of an individual; and

(b) a health service to be provided to the individual.

21.2.2 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 25.

21.2.3 Accordingly, a School may trigger the health information provisions 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 pupils health, diagnoses a pupil's illness or disability, or treats a pupil. The provisions are not intended to apply where, for example, a member of School staff carries out emergency first aid on a pupil. Schools sometimes employ professionals to supply health services and sometimes, in effect, provide such services through their regular teaching staff.

21.2.4 If a School is unsure as to whether it is providing a 'health service', it should treat the health information with the higher level of protection afforded by the health information provisions. These are discussed below.

21.3 Collection of Health Information

21.3.1 Health information generally should only be collected:

(a) with the consent of the pupil or parent;

(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.

21.3.2 In most cases in Schools, the collection will be with the consent of the individual or, in the case of pupils, 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 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 pupil with a disability or health problem from another School.

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

21.4 Use or Disclosure of Health Information

21.4.1 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.

21.4.2 Health information of a pupil should not be disclosed to third parties, such as to another parent or an organisation or school which has temporary care of the pupil unless the School considers that it is reasonably necessary to disclose it to ensure that the health or safety of the pupil is maintained.

21.4.3 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.

21.4.4 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.

21.4.5 Difficult issues may arise where a School becomes aware of health information about a pupil which the pupil 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.

21.5 Health Information and Employees

21.5.1 As discussed at Section 24, 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.

21.5.2 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). 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.

21.6 Additional Requirements in States and Territories

21.6.1 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 15 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.

21.6.2 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 a parent or guardian, may act on their behalf.

21.6.3 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 Act applies to persons who have been deceased for a period of 30 years or less, as well as small business operators. As noted above, the Act also applies to information contained in employee records.

21.6.4 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 complainant. 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 representative (such as a parent or guardian) of the child may exercise the right to make that request.

21.6.5 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.

21.6.6 Additionally, the Act provides that a right or power conferred upon a young person (being a person under 18 years of age, *other than* a person who is of sufficient age and mental and emotional maturity to understand the nature of and give consent to a health service) by the Act is exercisable only by a guardian of the young person, and is not exercisable by a young person on their own behalf.

21.7 Inconsistencies between Federal and State laws

21.7.1 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 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.

21.7.2 While the principles in New South Wales, Victoria and the Australian Capital Territory legislation were based on the NPPs, they are not identical, and in some cases impose different 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.

21.7.3 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.

22. CLOUD COMPUTING

22.1.1 Many organisations including schools in Australia are now making use of 'cloud computing' services. In broad terms these are services that are delivered over a network which provide computing resources, both hardware and software.

22.1.2 Importantly, from a School's point of view, it entrusts the cloud service provider with the School's data. Cloud resources are utilised to reduce IT operational costs.

22.1.3 The cloud service may offer a range of IT and security services that the School may not have at a more affordable price. However cloud computing also carries with it risks, as the School that uses the cloud is reliant upon the cloud provider maintaining the security of the data and maintaining it so that it can be accessed by the School as required. Experience has shown that there are some significant instances of hacking of data contained in the cloud.

22.1.4 In addition many cloud providers store data offshore, often in multiple locations, including overseas.

22.1.5 Under the Privacy Act, a School that uses cloud computing facilities located offshore will in many instances be held responsible for any loss, unauthorised access, or unauthorised disclosure of personal information (**Data Breach**) by the cloud service provider (see Section 11).

22.1.6 If a School or System is considering using cloud storage, it should consider a number of issues including:

(a) the sensitivity of the data from a privacy perspective;

(b) the sensitivity of the data from a business operational perspective;

(c) whether it is permitted to send the data offshore, in other words, have people been informed that their personal information may be sent offshore (however, see our comment below at 22.1.9);

(d) in what jurisdictions the data may be stored by the cloud provider and whether it could be stored on servers in Australia;

(e) is the data encrypted when transferred and stored;

(f) what other forms of security and data back up does the provider use; and

(g) who is to notify the Information Commissioner and affected individuals if there is an eligible data breach (**EDB**) under the notifiable data breaches scheme (**NDB Scheme**) (see Section 26).

22.1.7 It will be important where confidential information is to be held in the cloud that the cloud provider is subject to strict contractual provisions that:

(a) place stringent conditions on the cloud provider to maintain security of the data and accept responsibility for any breach;

(b) allow the School to withdraw the information at any time;

(c) prevent the cloud provider from using, disclosing or processing any information other than for the purpose of providing the cloud service;

(d) prevent the cloud provider from retaining any information when it is withdrawn; and

(e) ensure the cloud provider will notify the School if there is a Data Breach and provide assistance to the School in responding to any Data Breach (including in relation to gathering the information required for notification to the Information Commissioner and individuals if there is an EDB under the NDB Scheme).

22.1.8 Providers of cloud computing services offer different levels of contractual protection to customers. It is suggested that specialist advice is obtained and a risk assessment is carried out prior to entering into contracts with providers.

22.1.9 The use of a cloud service provider by a School *may* trigger the requirements under APP 6 relating to disclosure and APP 8 relating to cross-border disclosure, and associated obligations relating to notification of disclosure in a School's privacy policy and collection notices. However, these APPs only apply to *disclosure* of personal information. The APP Guidelines provide that where a School provides personal information to a cloud service provider located overseas, the provision of the information may be a '*use*' and not a '*disclosure*' where:

(a) the information is provided for the limited purpose of performing the services of storing and ensuring the School may access the personal information;

(b) 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;

(c) the contract requires any sub-contractors to agree to the same obligations; and

(d) the contract between the School and the cloud service provider gives the School effective control of the information. Issues to consider include whether the School retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, the security measures that will be used for the storage and management of the personal information, and whether the personal information can be retrieved or permanently deleted by the School when no longer required or at the end of the contract.

23. CREDIT PROVIDERS

23.1 Schools as credit providers

23.1.1 Schools may be recognised as 'credit providers' under the Privacy Act. 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.

23.1.2 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.

23.1.3 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.

23.1.4 The Privacy Commissioner 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.

23.1.5 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".

23.1.6 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.

23.1.7 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 APP1 as explained further in Section 6 of the Manual.

23.1.8 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 (eg 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.

23.1.9 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 Paragraph 23.1.8 they only need to state in their privacy policy "The School does not collect personal information from their credit providers or credit reporting bodies".

23.1.10 The AIS and CEC has received more detailed external legal advice on this issue. If a School is concerned about these provisions, it should contact Charles Alexander on (02) 9299 2845 or at calexander@aisnsw.edu.au, or Ian Baker on (02) 9287 1520 or at Ian.Baker@cecnsw.catholic.edu.au for more information.

24. EMPLOYEE RECORDS

24.1 Employee Records

24.1.1 An act done, or practice engaged in, by an APP Entity 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 employer and the individual; and

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

24.1.2 An 'employee record' is defined broadly to be a record of personal information relating to the employment of an employee. Examples of this type of information include the terms and conditions of employment, personal contact details, performance and conduct, disciplining, salary, termination and trade union membership.

24.1.3 The employee records exemption does not extend to prospective employees, contractors, consultants or volunteers. In New South Wales the health records of an employee 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 this applies to your School, see Section 21.

24.1.4 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 collecting, 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 it is not collected by their employer.

24.1.5 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).

24.1.6 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.

24.1.7 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.

24.1.8 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 15). 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.

24.1.9 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. Under the Privacy Act, examples of employee records include health information about an employee and personal information about any or all of the following:

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

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

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

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

(e) the employee's performance or conduct;

(f) the employee's hours of employment;

(g) the employee's salary or wages;

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

(i) the employee's trade union membership;

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

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

24.1.10 Some practices in relation to employees could possibly fall outside the employee records exemption. For example, a record of a staff member's place of birth (collected via a 'Banking Information Form') might not be directly related to the employment relationship and therefore not within the 'employee records' exemption.

24.1.11 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.

24.1.12 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.

24.1.13 If employee records are given to related organisations, no collection notice need be given, but the employee exemption will not apply in the hands of that related organisation.

24.2 Recommendation

24.2.1 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.

24.2.2 If employee records are given to related organisations no collection notice need be given, but the employee exemption will not apply in the hands of that related organisation.

24.2.3 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.

24.2.4 Information provided to a central Catholic Education Office by 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.

25. SCHOOL COUNSELLORS

25.1 General

25.1.1 From time to time issues arise in relation to the role of School Counsellors and their obligations to pupils, the schools at which pupils are enrolled and the parents of those pupils. Other issues arise relating to the operation of the Privacy Act in relation to the record of personal information which is collected by Counsellors. These notes address these issues in the context of this Manual**.**

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

(a) Counsellors do not enjoy any general 'legal professional privilege';

(b) Counsellors must respond to Summons and Subpoenas (subject to Protected Confidences provisions, as set out immediately below);

(c) Counsellors have to maintain the confidence of their clients in the context of an ethical (not just a legal) relationship;

(d) Protected Confidences in NSW:

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.

Specifically, the court can order the production of the material if satisfied of the following:

(i) the documents have substantial probative value, ie. they will provide significant assistance in establishing particular facts;

(ii) other evidence of the protected confidence or the contents of the document is not available; and

(iii) the public interest in disclosing the documents outweighs the public interest in keeping them confidential. In assessing the public interest of disclosing the documents, the court must take into account the likelihood and nature or extent of harm that would be caused to the alleged victim; and

(e) also, the definition of counselling means that it is possible that communications between victims of sexual assault and school personnel, in addition to specialist counsellors, may be subject to the protected confidence provisions.

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

25.2 School Counsellors Generally

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

25.3 Professional Associations

25.3.1 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.

25.3.2 Often, necessary information can be conveyed to a person (ie. 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 which relates to the well being of a pupil of the school.

25.3.3 In this context reference should also be made to Section 9 of this Manual which deals with 'Use or Disclosure of Personal Information'.

25.4 Effect of Employment Status of Counsellors

25.4.1 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 Principal is able to call for those records which directly pertain to a pupil 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 pupil 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 15 of this Manual.

25.4.2 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. However, as schools from time to time will require reports from the Counsellor about pupils 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 could form part of the general collection notice given by the school. Thus the collection notice may include a paragraph to the effect:

> *'The School contracts with an external service provider [or name] to provide counselling services for pupils. The Principal may require the Counsellor to inform him or her or other teachers of any issues the Counsellor believes may be necessary for the School to know for the well-being or development of the pupil who is counselled or other pupils at 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 pupils 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 pupil or pupils concerned or take action to prevent harm to the pupil. 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 Counsellor may be able to be accessed by the pupil. Records held by the School which came from the Counsellor would be liable to be provided by the School to the pupil on request, subject of course to any exemptions contained in the APPs as mentioned earlier. (See Section 9 'Use or Disclosure of Personal Information')

25.4.3 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 pupil, or as requested by the parents.

25.5 Does it matter who referred the pupil to the Counsellor?

25.5.1 Generally, this makes no difference to the position set out above. However, it is likely that the person making the referral may seek a report from the Counsellor. Where the Counsellor is a private practitioner the consent of the pupil (or in this case of a young pupil, the parent) would be required before that report could be provided. Where the Counsellor is an employee of the School or a contractor to the School, the School would not need the consent of the pupil before providing a report to the parents, provided that it could be established that the report was a related secondary purpose (or directly related, if health information) to providing schooling to the pupil and disclosure would be reasonably expected. This expectation would be dealt with through the 'collection notice'. Even if this were not the case disclosure to the parent may be necessary for the School to fulfil its duty of care, as discussed below.

25.5.2 However it is important that all pupils using the School's counselling service are made aware that there will be occasions when the contents of discussions may be disclosed to the Principal (and possibly others) and that the Principal may wish to see the Counsellor's records. A draft form of Disclosure Statement to Students is attached at Annexure 4.

25.5.3 If the pupil is thought to be of an age or maturity that they would not understand that they are consenting to this disclosure, should it be necessary, then the parents or guardian of the pupil should be given the notice. In determining whether this is necessary regard should be had to Section 17 'Consent and Young People'. There may be times when this would be inappropriate, in which case the matter should be discussed with the Principal.

25.6 Duty of Care

25.6.1 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 pupil suffers injury as a result, the School may be found to be vicariously liable for the activity of that Counsellor. If a pupil 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.

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

25.6.3 The issue of Duty of Care is referred to in Section 18 of this Manual. 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 related secondary purpose which is reasonably expected; or

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

However, on occasions, even though disclosure to parents may be permitted, for example, as a reasonably expected 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.

26. RESPONDING TO DATA BREACHES

26.1 Introduction

26.1.1 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**).

26.1.2 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 use or disclosure of personal information which is not permitted under APP6 (see ' Section 9 – Use or disclosure of personal information). 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;

(d) loss or theft of hard copy documents; and

(e) misuse of personal information of students or parents by School personnel.

26.1.3 From 22 February 2018, all agencies and organisations with existing personal information security obligations under the Privacy Act, including Schools, will be required to report certain data breaches under the notifiable data breaches scheme (**NDB Scheme**). The NDB Scheme was inserted into the Privacy Act by the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth). It sets out obligations to notify affected individuals and the Information Commissioner about data breaches which fall within the definition of an 'eligible data breach' (**EDB**).

26.1.4 A Data Breach is an 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 Information Commissioner. However, in some cases, a School may decide to voluntarily notify individuals and/or the Information Commissioner. There are also limited exceptions to notifying affected individuals and the Information Commissioner of an EDB in certain circumstances.

26.1.5 This Section 26 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 Information Commissioner of an EDB and notifying individuals affected by an EDB, and potential exceptions to notification; and

(d) reviewing the Data Breach/EDB.

An adapted version of the OAIC Data Breach Response Summary setting out these steps is included in Annexure 6.

26.1.6 Additional useful resources:

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

(b) the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) (**Amending Act**); and

(c) the explanatory memorandum for the Privacy Amendment (Notifiable Data Breaches) Bill (**Explanatory Memorandum**).

26.2 Containing the Data Breach

26.2.1 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. 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.

26.3 Assessing whether the Data Breach is an EDB

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

(a) 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.

26.3.2 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 Information Commissioner – not every Data Breach. EDBs will be Data Breaches:

- that a reasonable person in the School's position (rather than the individual to whom the information relates or any other person) would conclude,
- based on all of the information either immediately available to them, or available following reasonable inquiries or an assessment of the data breach,
- that the unauthorised access to or disclosure of the particular personal information or 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.

26.3.3 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 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 8.

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 Information Commissioner was also notified.

26.3.4 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 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 in relation to any remedial action. 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; or

(iii) 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 fund raising 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 Information Commissioner 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.

26.3.5 Timing of the assessment

(a) If Schools suspect an EDB may have occurred, they should take reasonable steps to conduct this assessment expeditiously, and where possible, within 30 days after the suspicion arises that a Data Breach has occurred. A sample data breach response plan is set out in Annexure 8.

26.3.6 What if multiple organisation are involved in the EDB or suspected EDB?

(a) If a School or other organisation (eg a cloud service provider or other third party supplier) are together involved in a Data Breach affecting personal information of individuals the School handles, and either the School or other organisation has made an assessment about a 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 Information Commissioner. 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 Information Commissioner 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 the basis that it is an EDB and, notifies parents whose information was involved and the Information Commissioner.

26.4 Notifying individuals and the Information Commissioner

26.4.1 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 Information Commissioner in accordance with the OAIC *Notifiable Data Breach statement – Form* – this can be emailed or lodged online via the OAIC website; and

(c) notify individuals of this statement as soon as practicable after notifying the Information Commissioner.

26.4.2 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 Information Commissioner and individuals, as explained below.

26.4.3 The NDB Scheme provides three options for notifying affected individuals of the statement provided to the Information Commissioner:

(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 Information Commissioner on its website if it has one and take reasonable steps to publicise the contents of the statement.

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

26.4.5 Where the individual being notified is a pupil, it may be appropriate to notify the parent or guardian instead of or as well as the pupil. The age and maturity of the pupil 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 17.

26.4.6 Schools can tailor the notification to individuals, as long as it includes the content of the statement Schools must provide to the Information Commissioner. The NDB Scheme required 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 (eg the School) that has reasonable grounds to believe the EDB has happened;

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

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

26.4.7 There are limited relevant exceptions to Schools' obligations to notify the Information Commissioner 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; and

(b) where the Information Commissioner 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 Information Commissioner or some or all of the individuals should not be made or delayed.

26.4.8 Whilst not mandatory, 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 – eg 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 (eg professional bodies, or the ATO if Tax File Numbers are affected); and

(d) the Australian Cyber Security agencies such as the ACS Centre, including National Computer Emergency Response Team (**CERT**) or the Australian Cyber Crime Online Reporting Network (**ACORN**) – 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.

26.5 Reviewing the Data Breach/EDB

26.5.1 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 staff training staff.

26.6 Consequences

26.6.1 The NDB Scheme is subject to the existing regulatory and enforcement framework overseen by the Information Commissioner 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 Information Commissioner into the causes of the Data Breach/EDB and the School's response;

(b) a determination by the Information Commissioner that the School take specified steps to remedy noncompliance, perform any reasonable act to redress any loss suffered, pay monetary compensation;

(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 Information Commissioner to court to impose a civil pecuniary penalty of up to $2.1 million per breach.

26.7 Voluntary notification

26.7.1 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 the Information Commissioner 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 14) 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 publically 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.

Example:

A Year 7 co-ordinator asks members of the IT Team if they can assist in mapping new Year 7 student's home addresses to the most viable bus route using Google Maps, so as to assist the students in their transition to high school. The IT staff member assists by exporting the Year 7 students' home address from the school information system and uploads them to Google Maps and then attempts to map their most direct bus route to and from school. However, the Year 7 co-ordinator and IT staff member do not seek authorisation to do this from the Principal nor the parents of each student. The IT staff member inadvertently uploads the students home addresses without any privacy settings so that when a member of the public performs a search using a student's name and school, the search results display a link to a map of that student's travel route to school, including their full name and home address. Subsequently an irate parent contacts the school concerned that their child's home address is publicly available on the Internet. The Director of IT is informed. The school subsequently sends a letter to all affected parents advising them of the breach and the action it has taken to re-secure the student's home addresses. The school also reviews the school data security policy and the IT Team and teachers take part in privacy training. The School may also have been using the students' information for a purpose not permitted by APP6 (see Section 9).

ANNEXURE 1 – SUMMARY OF A SCHOOL'S OBLIGATIONS IMPOSED BY THE AUSTRALIAN PRIVACY PRINCIPLES

1. Manage personal information in an open and transparent way.
2. 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 compliance with the APPs; and
   (b) will enable the School to deal with inquiries or complaints about compliance with the APPs.
3. Have a clearly expressed and up-to-date Privacy Policy about the School's management of personal information.
4. If it is lawful or practicable, give individuals the option of interacting anonymously with the School or using a pseudonym.
5. Only collect personal information that is reasonably necessary for the School's functions or activities.
6. Obtain consent to collect sensitive information unless specified exemptions apply.
7. Use fair and lawful means to collect personal information.
8. Collect personal information directly from an individual if it is reasonable and practicable to do so.
9. If the School receives unsolicited personal information, determine whether it could have collected the information under APP 3 as if it had solicited the information. If so, APPs 5-13 will apply. If not, the information must be destroyed or de-identified.
10. 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:
    (a) why the School is collecting information about them;
    (b) who else the School might give it to; and
    (c) other specified matters.
11. 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 it from someone else.
12. 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).
13. 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.
14. Do not use personal information for direct marketing, 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).

15. Before the School discloses personal information to an overseas recipient it must take such steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs, unless an exception applies.

16. Government related identifiers must not be adopted, used or disclosed unless one of the exceptions applies (eg. the use or disclosure is reasonably necessary to verify the identity of the individual for the purposes of the School's functions or activities).

17. 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. This may require the School to correct the information and possibly advise organisations to whom it has disclosed the information of the correction.

18. Take such steps as are reasonable in the circumstances to protect the personal information the School holds from misuse, interference and loss and from unauthorised access, modification or disclosure.

19. Take such steps as are reasonable in the circumstances to destroy or permanently de-identify personal information no longer needed for any purpose for which the School may use or disclose the information.

20. If requested, the School must give access to the personal information it holds about an individual unless particular circumstances apply that allow it to limit the extent to which it gives access.

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

ANNEXURE 2 - PRIVACY POLICY

1.1 Privacy Policies

1.1.1 A Privacy Policy is needed to inform individuals about the practices of the School in relation to personal information. It also serves as a guide to the School's staff as to the standards to be applied in respect of handling personal information and ensure consistency in the School's approach to privacy.

1.1.2 The following two draft Privacy Policies are intended to allow the School to satisfy the requirements of APP 1.4, dealing with openness. The first Privacy Policy is designed for non systemic Schools and the second is designed for systems and Schools operating within systems.

1.1.3 The Privacy Policy which the School adopts may be used, in conjunction with the collection notices, to satisfy the requirements in APP 5.2 to ensure that individuals are aware of relevant matters on collection of personal information.

1.1.4 The Privacy Policies are drafts only and must be adapted to reflect each School or system's particular acts and practices.

Sample Privacy Policy (AIS schools)

This Privacy Policy sets out how the School manages personal information provided to or collected by it.

The School is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988*. 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**)]].

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.

What kinds of personal information does the School collect and how does the School collect it?

The type of information the School collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School, including: [***insert the following as relevant, and add any other general kinds of information***]
    - name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
    - parents' education, occupation and language background;
    - medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
    - 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 court orders;
    - volunteering information; and
    - photos and videos at School events;
- job applicants, staff members, volunteers and contractors, including: [***insert the following as relevant, and add any other general kinds of information***]
    - 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;
    - medical 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;
- 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.

Personal Information you provide: The School will generally collect personal information held about an individual by way of forms filled out by Parents or pupils, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than Parents and pupils provide personal information.

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 or a reference from another school.

Exception in relation to employee records: 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 an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and 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.]

How will the School use the personal information you provide?

The School will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected by you, or to which you have consented.

Pupils and Parents: In relation to personal information of pupils and Parents, the School's primary purpose of collection is to enable the School to provide schooling to pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the School. This includes satisfying the needs of Parents, the needs of the pupil and the needs of the School throughout the whole period the pupil is enrolled at the School.

The purposes for which the School uses personal information of pupils and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration of the School;
- looking after pupils' educational, social and medical wellbeing;
- seeking donations and marketing for the School; and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

In some cases where the School requests personal information about a pupil or Parent, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

Job applicants and contractors: In relation to personal information of job applicants and contractors, the School's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor, as the case may be.

The purposes for which the School uses personal information of job applicants and contractors include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking donations and marketing for the School; and
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Volunteers: The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as [alumni associations], to enable the School and the volunteers to work together.

Marketing and fundraising: The School treats marketing and 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 pupils and staff thrive. Personal information held by the School may be disclosed to organisations that assist in the School's fundraising, for example, the School's Foundation or alumni organisation [or, on occasions, external fundraising organisations].

Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

Who might the School disclose personal information to and store your information with?

The School may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools;
- 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;
- 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);
- people providing administrative and financial services to the School;
- recipients of School publications, such as newsletters and magazines;
- pupils' 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.

Sending and storing information overseas: The School may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

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. 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)*]

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

The School's staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals.

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.

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 and obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. Pupils will generally be able to access and update their personal information through their Parents, but older pupils 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 or to update any personal information the School holds about you or your child, please contact the [School Principal] or [School Administrator] by telephone or in writing. The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is

extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of pupils

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 pupil to the pupil's Parents. The School will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.

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. However, there may be occasions when access is denied. Such occasions would include 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 pupil.

The School may, at its discretion, on the request of a pupil grant that pupil access to information held by the School about them, or allow a pupil 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 pupil and/or the pupil'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 please contact the [School Principal] by writing 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 applicable

Sample Privacy Policy

[Catholic Education Office of the […] Diocese / …System]

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 provided to or collected by it.

The [CEO / System] is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988*. In relation to health records the [CEO / System] is 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**)]].

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.

What kinds of personal information does a school collect and how does a school collect it?

The type of information schools collect and hold includes (but is not limited to) personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians (**Parents**) before, during and after the course of a pupil's enrolment at the school [***insert the following as relevant, and add any other general kinds of information***]
    - name, contact details (including next of kin), date of birth, gender, language background, previous school and religion;
    - parents' education, occupation and language background;
    - medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
    - 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 court orders;
    - volunteering information; and
    - photos and videos at school events;
- job applicants, staff members, volunteers and contractors, including: [***insert the following as relevant, and add any other general kinds of information***]
    - 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;

- medical 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;
- 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.

Personal Information you provide: A school will generally collect personal information held about an individual by way of forms filled out by Parents or pupils, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than Parents and pupils provide personal information.

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 or a reference from another school.

Exception in relation to employee records: Under the Privacy Act [***insert the following NSW:*** and the Health Records Act**]**, the Australian Privacy Principles [***insert the following in NSW:*** and Health Privacy Principles] do not apply to an employee record. As a result, this Privacy Policy does not apply to the school's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the school and employee. [***insert for Vic and ACT*** The school handles staff health records in accordance with the Privacy Principles in the Health Records Act.]

How will a school use the personal information you provide?

A school will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

Pupils and Parents: In relation to personal information of pupils and Parents, a school's primary purpose of collection is to enable the school to provide schooling to pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the school. This includes satisfying the needs of Parents, the needs of the pupil and the needs of [the CEO / System] and school throughout the whole period the pupil is enrolled at the school.

The purposes for which [the CEO / System] and a school uses personal information of pupils and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration;
- looking after pupils' educational, social, spiritual and medical wellbeing;
- seeking donations and marketing for the school; and
- to satisfy the [CEO's / System's] and the school's legal obligations and allow the school to discharge its duty of care.

In some cases where a school requests personal information about a pupil or Parent, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

Job applicants and contractors: In relation to personal information of job applicants and contractors, a school's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor, as the case may be.

The purposes for which a school uses personal information of job applicants and contractors include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the school; and
- satisfying the [CEO's / System's] and the school's legal obligations, for example, in relation to child protection legislation.

Volunteers: A school also obtains personal information about volunteers who assist the school in its functions or conduct associated activities, such as [alumni associations], to enable the school and the volunteers to work together.

Marketing and fundraising: Schools treat marketing and 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 pupils and staff thrive. Personal information held by a school may be disclosed to an organisation that assists in the school's fundraising, for example, the school's Foundation or alumni organisation [or, on occasions, external fundraising organisations].

Parents, staff, contractors and other members of the wider school community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

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]. This allows schools to transfer information between them, for example, when a pupil transfers from a [CEO / System] school to another school conducted by the [CEO / System].

Who might a school disclose personal information to and store your information with?

A school may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools;
- government departments (including for policy and funding purposes);
- the CEO, the Catholic Education Commission (**CEC**), the school's local diocese 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;
- 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);
- people providing administrative and financial services to the school;
- recipients of school publications, such as newsletters and magazines;
- pupils' 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.

Sending and storing information overseas: A school may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, a school will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

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. 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 and their 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 Diocese / System, replace this paragraph with one relevant to the platform used by the Diocese / …System(e.g. Microsoft 365)***]

How does a school treat sensitive information?

In referring to 'sensitive information', a school means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

The [CEO's / System's] and the schools' staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals.

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.

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 and obtain access to any personal information which the [CEO / System] or a school holds about them and to advise the [CEO / System] or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Pupils will generally be able to access and update their personal information through their Parents, but older pupils 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 or to update 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 telephone or in writing.

The school may require you to verify your identity and specify what information you require. The school may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the school will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of pupils

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 pupil to the pupil's Parents. A school will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.

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. However, there may be occasions when access is denied. Such occasions would include 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 pupil.

A school may, at its discretion, on the request of a pupil grant that pupil access to information held by the school about them, or allow a pupil 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 pupil and/or the pupil'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, please contact the [school's Principal] by writing 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 applicable

ANNEXURE 3 - 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[1]	Disclosed outside School?
KEY:	**Y/N**	**PA=Parent PU=Pupil 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 pupil enrolled B=Up to 6 years after pupil leaves C= Up to 10 years after pupil 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[2]							
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							

[1] Considering the nature of the information, type of storage, access and possible disclosure
[2] For example, government welfare agencies/departments.

Photos, video							
Employment information							
Legal case files							

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[3]	Disclosed outside School?
KEY:	**Y/N**	**PA=Parent PU=Pupil 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 pupil enrolled B=Up to 6 years after pupil leaves C= Up to 10 years after pupil 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							
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							

[3] Considering the nature of the information, type of storage, access and possible disclosure

PERSONAL INFORMATION TEMPLATE – Employee

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[4]	Disclosed outside School?
KEY:	**Y/N**	**PA=Parent PU=Pupil 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 pupil enrolled B=Up to 6 years after pupil leaves C= Up to 10 years after pupil 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							
Next of kin							
Emergency contact numbers							
Names of doctors							
Job application, LOA							
Professional development history							
Appraisal information							
Details of disability							
Bank details							
Pay advices							
Complaint records							
Communication with parents/carers							
Referee names, contact numbers							
Role description							
Leave details							
Medical certificates							
Employment file notes							
Diary entries							
Superannuation details							
Case management notes							
Photos, video							
Employment information							
Workplace surveillance information							
Workplace emails							

[4] Considering the nature of the information, type of storage, access and possible disclosure

Private emails							
Internet browsing history							
Investigation reports							
Legal case files							

ANNEXURE 4 – DISCLOSURE STATEMENT TO STUDENTS

Counselling at xxx School – Things You Should Know

The School provides counselling services for its students as part of its pastoral care program. These are provided through counsellors employed by the School.

Students are encouraged to make use of these services if they need assistance. There are however a number of things that students and their parents should know before using the counselling service.

1. Records will be made of counselling sessions and because the counsellor is an employee, those records belong to the school, not the counsellor.

2. The School is very conscious of the need for confidentiality between counsellor and student. However at times it may be necessary for the Counsellor to divulge the contents of discussions or records to the Principle if the Principal or the Counsellor considers it necessary for the student's welfare to discharge the school's duty of care to the student.

3. It is also possible that the Principal may need to disclose aspects of discussions with counsellors to others in order to assist the student.

4. Where a disclosure is made it would be limited to those who need to know, unless the students consents to some wider disclosure.

We emphasise that disclosures (if any) would be very limited. However if a student is not prepared to use the counselling services on the basis set out above the student will need to obtain counselling services from outside the school.

ANNEXURE 5 – PHOTOGRAPH/VIDEO PERMISSION FORM

[NAME of SCHOOL]

PHOTOGRAPH/VIDEO PERMISSION FORM

Insert School logo here

Dear Parent/Guardian

At certain times throughout the year, our students may have the opportunity to be photographed/filmed for our school publications, such as the school's newsletter or external school websites and social media sites, or to promote the school in newspapers and other media.

The [***insert relevant educational authority, eg: [name of system or School]/ Catholic Education Commission of*** [and the [***xx***] Diocese (**Diocese**)] may also wish to use student photographs/videos in print and online promotional, marketing, media and educational materials.

We would like your permission to use your child's photograph/video for the above purposes to which you agree. Please complete the permission form below, include a mark next the uses you consent to, and return to the school as soon as possible.

Thank you for your continued support.

STUDENT'S NAME: _____ **YEAR LEVEL:** _____

NOTE: Please confirm your consent to the uses described below by ticking the relevant box. If you do not want your child's name used please delete "and name". If you do not wish your child's image to be used in the way described below you can leave the box blank.

- I give my consent to the School using my child's photograph/video:
  - ☐ on the school website – with name
  - ☐ on school social media sites – with name
  - ☐ in materials promoting the school, including advertising materials – with name
  - ☐ in newspapers and other media to promote the school's activities – with name
- I give my consent to the [***system***]/[***CECNSW/Diocese***] using my child's photograph/video:
  - ☐ in material available free of charge to schools and education departments around Australia for the [system]/[***CECNSW/Diocese***]'s promotional, marketing, media and educational purposes without acknowledgment, remuneration or compensation.
- I understand and agree that if I wish to withdraw any consent provided above, it is my responsibility to notify the school.

Licensed under NEALS: The photograph/video may appear in material which will be available to schools and education departments around Australia under the National Educational Access Licence for Schools (NEALS), which is a licence between education departments of the various states and territories, allowing schools to use licensed material wholly and freely for educational purposes.

Name of Parent / Guardian (please circle) _____

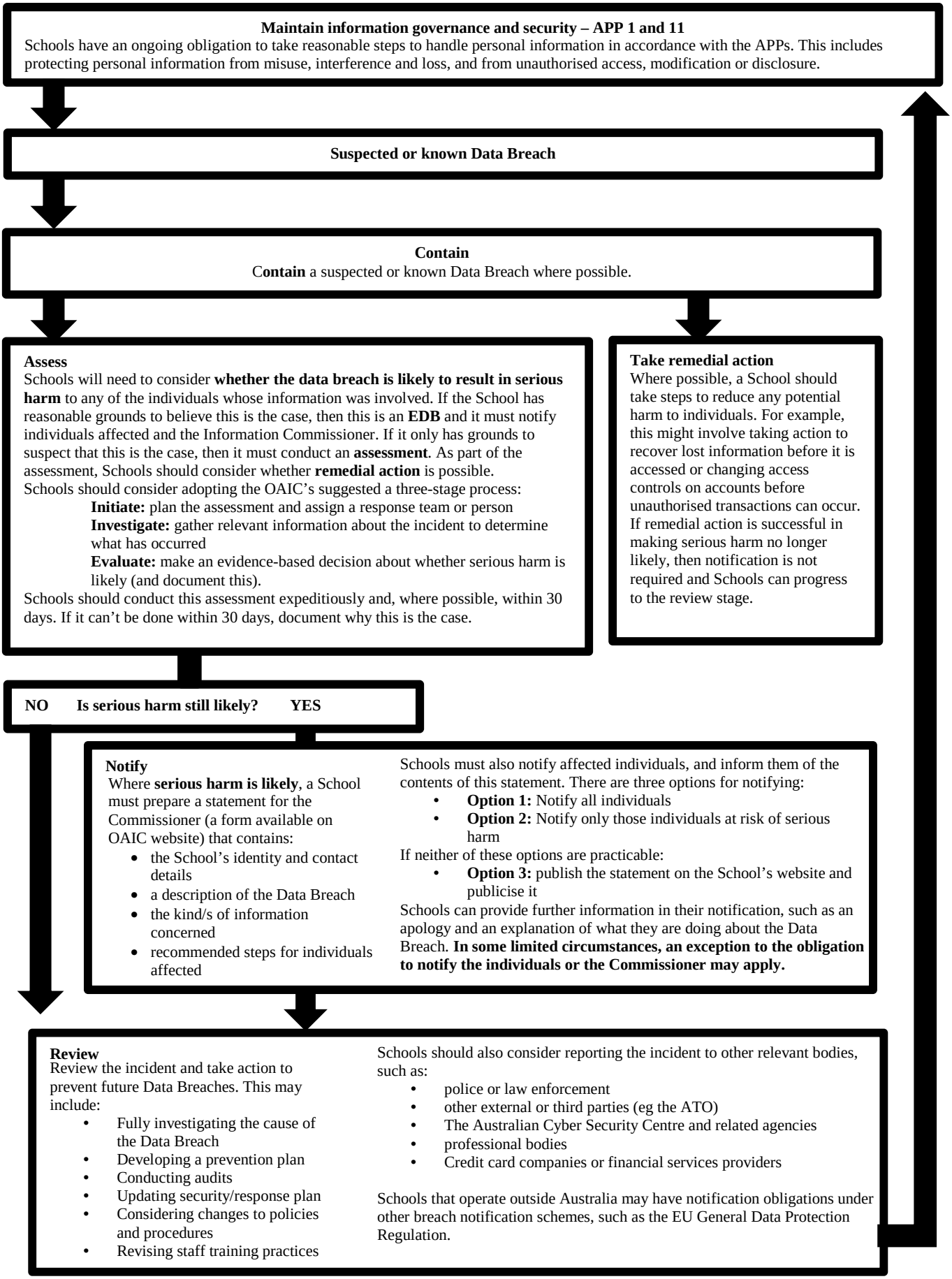
Signed: Parent/Guardian _____ Date: _____

If Student is aged 15+, student must also sign: Signed: Student _____ Date: _____

Any personal information will be stored, used and disclosed in accordance with the requirements of the Privacy Act 1988 *(Cth).*

OFFICE USE **Date of Photograph/Video: (month & year)**	

ANNEXURE 6 – MANDATORY NOTIFICATION OF ELIGIBLE DATA BREACHES SUMMARY



**This summary is a modified version of the OAIC Data Breach response summary available at www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme*

ANNEXURE 7 – DATA BREACH RISK ASSESSMENT FACTORS

Consider who the personal information is about	
Who is affected by the breach?	Are pupils, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a pupil'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 pupils who attend the School may not give rise to significant risk. However, the same information about pupils who have attended the School counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and address of pupils 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 pupil's name, address and grades without malicious intent (eg if the information is accidentally emailed to the teacher), the risk of serious harm to the pupil 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 (eg 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 pupils' domestic circumstances may be used to bully or marginalise the pupil 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	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?

personal information?	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.
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 pupils who attend the School may not be sensitive information. However, the same information about pupils 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 pupil number that only the School uses – this should be contrasted to a pupil 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?
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 pupil'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 pupils' domestic circumstances may be used to bully or marginalise the pupil 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?	Examples include loss of public trust in the School or AIS/CEC, 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 8 – 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 the Association of Independent Schools to which they belong. 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 26.

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.

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.

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.

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 Information Commissioner.
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.]