Catholic Schools Office
DIOCESE OF MAITLAND-NEWCASTLE

Privacy Management for Schools Procedure

APPLICABLE TO	All CSO, Diocese and school-based employees		
DOCUMENT OWNER	Director of Schools		
SCHOOL ACTIONS	School procedure – Each school is to adopt and maintain a privacy management procedure consistent with and aligned to the principles and practices outlined in the Privacy Policy.		
APPROVAL DATE	9 November 2018		
APPROVED BY	CSO Leadership Team		
LAST REVIEW DATE/S	2017	NEXT REVIEW DATE	2021
RELATED DOCUMENTS	Privacy Policy 2018 Annual Privacy Compliance Checklist for Schools Collection Notices: Standard, Employment Collection Notice, Enrolment Information Collection Notice, Volunteer/Contractor Collection Notice Complaints Resolution Policy Confidentiality Agreement – Employees Consent to Use Student Materials Data Breach Response Procedure Disclosure Statement to Students – Counselling Services Photograph/Video Permission Form (Students, Employees) Workplace Internet, Email and Network Usage Policy November 2016		

Purpose

This procedure sets out the responsibilities of all employees regarding managing information privacy and provides practical advice when collecting, securing, storing, accessing, amending, using and disclosing personal information.

For information regarding disposal of information collected by the CSO and its school, refer to the Records Retention Schedule for Schools and Service Areas.

Scope

This procedure applies to all staff and volunteers at the CSO and its diocesan schools and includes persons who have entered into a relationship with the CSO and its schools for a specified period, including contractors and consultants. This procedure is to be read in conjunction with the Privacy Policy.

Responsibilities

Director of Schools

The Director of Schools is responsible for ensuring the actioning of the Privacy Management Procedure and its compliance and that the implementation of the policy and associated procedure are adequately resourced.

CSO Leadership Team, Heads of Service and Principals are responsible for:

- Ensuring all staff are aware of and familiar with the Privacy Policy;
- Ensuring processes are compliant with the Australian Privacy Principles (APPs);
- assessing reported privacy breaches and/or consulting with the Policy and Compliance Officer to take necessary action.

Diocese General Counsel is the nominated privacy officer for the diocese.

All Employees, Contractors and Volunteers (Employees) must:

- be aware of the requirements for the protection of personal information;
- direct any privacy complaints to the Parent Liaison and Complaints Officer;
- report suspected privacy breaches to their supervisor, manager, principal or directly contacting the Policy and Compliance Officer;
- complete an annual induction and any training specified on privacy compliance.

Step by Step

STAFF TRAINING AND INDUCTION

1. On an annual basis, at the beginning of each year (and during the year as part of induction for new employees), staff are to be briefed by their Principal or manager on privacy compliance requirements and sign confidentiality agreement and permission forms.
2. The privacy briefing session should incorporate but not be limited to the following:
    - Circulation of the Privacy Policy, these procedures and Privacy Breach Response Procedure
    - Circulation of the current Employee Standard Collection Notice
    - Collection of the following forms signed by staff:
        - Confidentiality Agreement – Employees
        - Photograph/Video Permission Form – Employees
3. A Privacy Training Register is to be maintained to record staff participation (see Appendix 1).
4. Principals are to nominate a school privacy officer to work through the Annual Privacy Compliance Checklist – see Appendix 2. This is signed by the Principal and archived in the school's governance folder.

COLLECTION OF PERSONAL INFORMATION

When collecting personal information, employees are to:

- only collect personal information directly from the individual.
- only use approved forms, questionnaires, interviews, survey tools or other tools used to collect personal information, ensuring the information collected is required to carry out the tasks directly related to the functions and activities of the business unit or school.
- annually, provide relevant privacy collection notices to the individual on collection of their personal information (Student, Volunteer, and Employee, including photograph and video permission forms).
- undertake privacy impact assessments for projects or decisions that involve new or changed personal information handling practices (including implementing new technologies). The Office of the Australian Information Commissioner publishes a *Guide to undertaking privacy impact assessments* includes information on threshold assessments, which will help you determine whether a privacy impact assessment is necessary.

SECURITY OF PERSONAL INFORMATION

Employees must apply protection to the personal information they control by:

- protecting and securing personal information in both paper and digital formats and on mobile devices from loss, unauthorised access, use, modification or disclosure, and any other misuse.

  reporting any loss of personal information to their manager, director or principal.
- not emailing student personal information outside the CSO.

- Schools are to consider separating information into Restricted Access and General Access Records with indication in the General Access Record that a Restricted Access Record exists.

PROVISION OF PERSONAL INFORMATION

The CSO and diocesan schools publish details of the type of personal information they hold, for what purpose and use in the Privacy Policy.

An individual whose information is held by the diocese has the right to expect that any access is permitted only for authorised purposes.

Employees must:

- Refer requests by individuals to access and amend their personal information to the diocese General Counsel.
- when processing requests, undertake identity authentication to be satisfied as to the requestor's identity or the identity of the parent or guardian for an individual under 18 years, and their right to access or amend the personal information.
- where there is doubt about an individual's right to access or amend personal information, contact the diocese General Counsel.

CHECKING ACCURACY OF PERSONAL INFORMATION

Employees must check the accuracy, completeness and currency of personal information before use.

USE OF PERSONAL INFORMATION

Employees must only use personal information for the purpose for which it was collected, unless the individual concerned has consented to the use of the information for another purpose or an exception applies. Any approved use must be recorded in the individual's file or in the system where the personal information is stored.

DISCLOSURE OF PERSONAL INFORMATION

Assistant Directors or Principals have authority to consider and approve requests for disclosure of personal information. In doing so they must:

- ensure a request for disclosure of personal information is in writing and justifies why the information is required.
- ensure the individual concerned is aware of, or has consented to that disclosure.
- advise the recipient in writing to not use or disclose the personal information for a purpose other than the purpose for which it was provided.
- ensure the disclosure:
    - is necessary for certain types of law enforcement.
    - has reasonable grounds in existence to indicate that the use of this information is necessary.
    - lessens a serious and imminent threat to the life or health of that person.
- record decisions to disclose the information (including reasons for disclosure and the information disclosed).

PRIVACY COMPLAINTS

Employees must direct any privacy complaints to the General Counsel.

PRIVACY BREACH RESPONSE

Any employee who suspects a breach of privacy must report it to their supervisor, manager, or principal. The following are examples of when a Data Breach may occur:

- Loss of mobile devices, laptops or other equipment containing personal information.

- Cyber-attacks on the ICT systems, resulting in access to or theft of personal information.
- Accidental transmission of personal information such as student reports to unintended recipients via email.
- Loss or theft of hard copy documents.

The supervisor, manager or Principal will assess the breach and consult with the Policy and Compliance Officer to take necessary action. Refer to the Diocese **Data Breach Response Procedure**.

SPECIFIC DUTIES FOR THE SCHOOL

[Here schools can include their own procedures and who has responsibility for privacy compliance actions. The Annual Privacy Compliance Checklist can serve as a guide. For example:

- Who the delegated Privacy Officer is
- How and when Student Standard Collection Notices are issued to families at the beginning of each year
- Who completes the Privacy Impact Assessments
- How and when Photograph/Video Permission Forms for students are issued]
- Etc.

Appendices

APPENDIX 1: PRIVACY REGISTER FOR SCHOOLS

Catholic Schools
DIOCESE OF MAITLAND-NEWCASTLE

2018 Privacy Register for School Staff
Privacy Compliance Update and overview

Signing this register records your participation in the annual privacy overview for school staff.

DATE COMPLETED	
SCHOOL	
PRINCIPAL OR DELEGATE SIGNATURE	

The original of this register should be retained by the school for COSI purposes.

First Name	Surname	CSO Employee Number	Signature

APPENDIX 2: ANNUAL PRIVACY COMPLIANCE CHECKLIST FOR SCHOOLS

Catholic Schools
DIOCESE OF MAITLAND-NEWCASTLE

Annual Privacy Compliance Checklist for Schools

Schools can use this checklist as part of the school's annual privacy management plan. Tick off each item when covered. Checklist to be signed off by Principal and archived in the school's Governance folder.

Tick √	ITEM	ACTION
POLICY AND PROCEDURES Policies and procedures for the CSO are found in Policy Documents on MNWorks.		
	Privacy Policy	Schools are to follow the CSO system policy.
	Privacy Management Procedure – Schools	Schools are to write a local procedure that outlines how they manage privacy; update to your site and context as part of the annual review.
	Privacy Breach Response Procedure	Schools are to follow the CSO system procedure.
	Privacy Complaint: Internal Review Guidelines	Schools are to ensure they are familiar with this process and may issue the guidelines to individuals who want to make a privacy breach complaint.
	Australian Privacy Principles for Schools	Schools are to ensure they are familiar with and follow the APPs.
COLLECTION NOTICES Collection notices outline what personal information schools collect and how they use it.		
	Disclosure Statement to Students – Counselling Services	Published in school handbook
	Compass Standard Collection Notice 2018	Send to all families at start of year.
	Employee Standard Collection Notice 2018	Make available to all staff.
	Student Standard Collection Notice 2018	Send to all families at start of year.
	Enrolment Information Collection Notice 2018	Include in all enrolment packages.
FORMS AND TEMPLATES		
	Confidentiality Agreement for Employees	Signed by all employees and filed in personnel files.
	Consent to Use Student Materials Form	Signed by students and filed in student files.
	Meeting Record Template	Use to record meetings or discussions.
	Photograph/Video Permission Form – Employees	Signed by employees and filed in personnel files.
	Photograph/Video Permission Form – Students	Signed by parents/students and filed in student files.
	Privacy Impact Assessments – Students, Employees, Parents, Contractors/Volunteers	Use the templates to establish what information is available to whom.
	Privacy Register	Use to record participants in annual privacy compliance overview
REVIEW AND TRAINING		
	Appoint a Privacy Officer. This ensures that someone in the school is primarily responsible for integrating privacy obligations into existing practices, procedures and systems and promoting a culture where the personal information of individuals is protected in accordance with your obligations under the Privacy Act.	
	Ensure all direct marketing communications set out clear 'opt out' provisions.	
	Ensure all privacy practices, systems and procedures are secure and close any gaps.	
	Ensure complaints and incident management systems are working.	
	Train staff on privacy issues – have employees sign a Privacy Training Register on completion of the privacy compliance update at the beginning of the year or during induction.	

Principal Name:_____ Principal Signature: _____ Date:

APPENDIX 3: SUMMARY OF AUSTRALIAN PRIVACY PRINCIPLES

The APPs are structured to reflect the personal information lifecycle. They are grouped into five parts:

Part 1 — Consideration of personal information privacy (APPs 1 and 2)

Part 2 — Collection of personal information (APPs 3, 4 and 5)

Part 3 — Dealing with personal information (APPs 6, 7, 8 and 9)

Part 4 — Integrity of personal information (APPs 10 and 11)

Part 5 — Access to, and correction of, personal information (APPs 12 and 13).

The requirements in each of these principles interact with and complement each other. For example, when collecting personal information, an APP entity should consider the requirements in Part 2 as well as in Part 4 concerning the integrity of the information.

APP 1: Open and transparent management of personal information

Requires implementation of privacy practices, procedures and systems to ensure compliance with the remaining APPs and to enable the management of inquiries and complaints.

The Privacy Policy is to be made readily available.

APP 2: Anonymity and pseudonymity

APP 2 entitles individuals to the option of anonymity or using a pseudonym, except where impracticable or another prescribed exception applies.

APP 3: Collection of solicited personal information

APP 3, in summary:

- permits collection of personal information only where reasonably necessary for one or more of its legitimate functions or activities
- requires personal information to be collected directly from the individual to whom it relates, unless impracticable or another prescribed exception applies and
- requires the consent from an individual in order to collect that individual's sensitive information, or another prescribed exception applies.

APP 4: Dealing with unsolicited personal information

APP 4 requires a school that receives unsolicited personal information to determine whether it would otherwise have had grounds on which to collect it (i.e. under APP 3) and:

- where it does have such grounds, to ensure compliance with the remaining APPs or
- where it does not have such grounds, to destroy or de-identify the personal information (provided it is lawful and reasonable to do so).

APP 5: Notification of the collection of personal information

APP 5 requires notification to an individual, at or before the time of collection, of prescribed matters. Such matters include but are not limited to whether the individual's personal information is collected from any third parties, the purpose(s) of collection, to whom personal information is disclosed and the processes through which an individual can seek access and/or correction to their personal information, or otherwise complain about the way in which it is handled.

Compliance with APP 5 usually requires 'collection statements' to be included on or with forms through which personal information is collected. Such statements should refer and include a link to the privacy policy.

APP 6: Use or disclosure of personal information

APP 6 prohibits disclosure of personal information for a purpose other than the purpose for which it was collected, unless the individual consents, the individual would reasonably expect their personal information to be used for the secondary purpose, or another prescribed exception applies.

Such prescribed exceptions generally arise where the disclosure is necessary to protect someone's health or safety or is otherwise in the public interest.

APP 7: Direct marketing

APP 7 generally prohibits personal information to be used for direct marketing purposes unless the individual reasonably expects it, or consents to it, and prescribed 'opt out' processes are in place through which the individual can elect not to receive direct marketing communications (and the individual has not elected as such).

APP 8: Cross-border disclosure of personal information

APP 8 requires the taking of reasonable steps to ensure the an overseas recipient of the information does not breach the APPs. This usually requires the APP entity to impose contractual obligations on the recipient. There are exceptions to this obligation, including but not limited to where:

- the APP entity reasonably believes the overseas recipient is bound by a law or scheme that protects personal information in a substantially similar way to that of the APPs or
- the individual consents to the disclosure in the knowledge that such consent will negate the APP entity's obligation to ensure the overseas recipient does not breach the APPs.

APP 9: Adoption, use or disclosure of government related identifiers

APP 9 prohibits the adoption, use or disclosure of a government-related identifier unless:

- required or authorised by law
- necessary to verify an individual's identity and/or
- another prescribed exception applies.

Government-related identifiers are identifiers that have been assigned by a government agency including an individual's licence number, Medicare number, passport number and tax file number.

APP 10: Quality of personal information

APP 10 requires the taking of reasonable steps to ensure personal information is accurate, up-to-date and complete.

APP 11: Security of personal information

APP 11 requires the taking of reasonable steps to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure.

Personal information must be destroyed or de-identified if it no longer required (unless otherwise required to retain it by law).

APP 12: Access to personal information

APP 12 requires that an individual be provided, upon request, with access to their personal information unless a prescribed exception applies.

APP 13: Correction of personal information

APP 13 requires the taking of reasonable steps to correct personal information held upon request from an individual for correction or where it is otherwise satisfied, that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading. If a request for correction is refused, it needs to provide the individual with the reasons for the refusal. Where correction does occur, the APP entity may need to notify third parties to which the personal information, in its incorrect form, was disclosed.