Catholic Education
Diocese of Cairns
Learning with Faith and Vision

Policy

Directive No:	
Approval Date:	2016 (BoG 10/2016)
Previous Review Dates:	2006,2013, 2014, 2016
Next Review Date:	
Author:	MG&E (based on NCEC/NCISA Privacy Compliance Manual (August 2016)

Privacy Policy

(Incorporating Privacy Policy Statement and Information Collection Notice)

Purpose

This Privacy Policy applies to Cairns Catholic Education Services and all schools in the Diocese of Cairns. It sets out how CES and each school manage personal information provided to or collected by it.
Cairns Catholic Education Services 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.

Policy

Catholic Education in the Diocese of Cairns will manage personal information provided to or collected by it in accordance with the *Privacy Act* and the Australian Privacy Principles.
This will apply to all personal, sensitive and health information regarding parents/guardians, students, employees and prospective employees, volunteers and others with whom CES/schools may have contact. Personal information will only be collected, recorded and used to fulfil the education mission of Catholic Education in the Diocese of Cairns.
This policy will be operationally expressed through the Cairns Catholic Education Privacy Policy Statement (Attachment 1) and the enrolment Information Collection Notice (Attachment 2).

Rationale

Catholic Education in the Diocese of Cairns is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988* (the *Privacy Act).*

Consequences

This policy will:

- be expressed through the Cairns Catholic Education Privacy Policy Statement (Attachment 1) and the student enrolment Information Collection Notice (Attachment 2). The Policy Statement will be available on CES and school websites and freely available in printed form on request to CES or schools. The Information Collection Notice will be signed by parents/guardians as part of the enrolment agreement.
- inform mandatory training for all staff in the management of obligations to apply the Australian Privacy Principles (APPs). Guidance is provided (Attachment 3) outlining school obligations under the Australian Privacy Principles.
- Provide guidance to CES/schools in managing data breaches – noting the schools legal, moral and reputational obligations to effectively manage cases where data is breached. Attachment 4 provides a protocol for managing breaches.
- Provide guidance to CES/schools to ensure requests for the release of personal information are managed in accordance with the Australian Privacy Principles. Attachment 5 provides guidance in determining whether personal information can be disclosed.
- be reviewed for compliance by the CES/Diocesan designated Privacy Officer.

Reflection

- *Privacy Act 1988* and *the Privacy Amendment (Enhancing Privacy Protection) Act 2012*.
- National Catholic Education Commission & National Council of Independent Schools' Associations: Privacy Compliance Manual (April 2014) – available on the CES Staff Portal.
- Summary of a school's obligations imposed by the Australian Privacy Principles (APPs) – see Attachment 3

See also (Related Policies and Guidelines)

- Code of Conduct for Employees of Catholic Education, Diocese of Cairns
- Statement of Principles for Employment in Catholic Education, Diocese of Cairns

Attachment 1

Catholic Education in the Diocese of Cairns will apply its Privacy Policy and its obligations under the *Privacy Act* in accordance with the following policy statement:

CAIRNS CATHOLIC EDUCATION PRIVACY POLICY STATEMENT

Personal information collected by schools and method of collection

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:
    - name, contact details (including next of kin), date of birth, previous school and religion;
    - 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:
    - 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.

Surveillance and monitoring: Catholic Education Services and schools reserve the right to monitor all staff and student Information and Communication Technology user activity to ensure compliance with legal, ethical and acceptable use expectations. Generally, this will reflect the content of ICT user agreements for students, the separate policies on the acceptable use of ICT for staff and students, and for staff, the provisions of the Catholic Education Code of Conduct for Employees and the Statement of Principles for Employment in Catholic Education. Schools may also use video surveillance as part of school safety and security management.

Exception in relation to employee records: Under the Privacy Act, the Australian 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.

School use of 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 Cairns Catholic Education Services and school throughout the whole period the pupil is enrolled at the school.

The purposes for which Cairns Catholic Education Services 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 Cairns Catholic Education Services' 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 Cairns Catholic Education Services' 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 Cairns Catholic Education Services to share personal (but not sensitive) information with other schools conducted by Cairns Catholic Education Services. Other Cairns Catholic schools may then only use this personal information for the purpose for which it was originally collected by Cairns Catholic Education Services. This allows schools to transfer information between them, for example, when a pupil transfers from a Cairns Catholic school to another school conducted by Cairns Catholic Education Services.

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:

- other schools and teachers at those schools;
- government departments;
- Cairns Catholic Education Services, the Queensland Catholic Education Commission, the school's local diocese and the parish, other related church agencies/entities, and schools within other Dioceses;
- medical practitioners;
- people providing educational, support and health services to the school, including specialist visiting teachers, [sports] coaches, volunteers, counsellors and providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority;
- 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 and Cairns Catholic Education Services 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.

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

Cairns Catholic Education Services and school 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, an individual has the right to seek and obtain access to any personal information which Cairns Catholic Education Services or a school holds about them and to advise Cairns Catholic Education Services 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 Cairns Catholic Education Services or a school holds about you or your child, please contact the school's Principal or administration 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

Cairns Catholic Education Services 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 Cairns Catholic Education Services about them or their child by contacting the school Principal or administration 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 Cairns Catholic Education Services or a school manages the personal information it holds, or wish to complain that you believe that Cairns Catholic Education Services or a school has breached the Australian Privacy Principles, please contact the school Principal by writing or telephone. Cairns Catholic Education Services 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.

Attachment 2

CATHOLIC EDUCATION SERVICES (CES)
INFORMATION COLLECTION NOTICE

The following notice applies to all schools and colleges, and Catholic Education Services in the Diocese of Cairns.

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:

- other schools and teachers at those schools;
- government departments;
- Cairns Catholic Education Services, other schools, the local diocese and parish and related church agencies and Catholic Education Commissions (Queensland and National)
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, [sports] coaches, volunteers, counsellors and providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority;
- 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 Cairns Catholic Education Services Privacy Policy.

8. The Privacy Policy Statement, 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 Privacy Policy Statement 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 website. This may include photographs and videos of pupil activities such as sporting events, school camps and school excursions. The school will obtain permissions from the pupil's parent or guardian (and from the student if appropriate) if we would like to include such photographs or videos in our promotional material or otherwise make this material available to the public such as on the internet.

12. 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.

13. Catholic Education in the Diocese of Cairns is bound by the Privacy Act (1988) and has adopted the 13 Australian Privacy Principles (APPs). Our obligations are outlined in the Privacy Policy and Privacy Policy Statement which details practices and procedures for the use and management of the personal and sensitive information we collect and record. The policy and statement are available on our website http://www.cns.catholic.edu.au A printed paper copy is available on request.

14. As part of our obligations and duty of care. If we do not obtain the personal and sensitive information referred to above, we may not be able to enrol or continue to enrol your pupil.

Attachment 3

SUMMARY OF A SCHOOL'S OBLIGATIONS IMPOSED BY THE AUSTRALIAN PRIVACY PRINCIPLES (APPs)

Source: National Catholic Education Commission & National Council of Independent Schools' Associations: Privacy Compliance Manual (April 2014). Note: This is a summary only and NOT a full statement of obligations.

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 (e.g. the use or disclosure is reasonably necessary to verify the identity of the individual for the purposes of the school's functions or activities).

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.

Attachment 4

TEMPLATE PRIVACY BREACH RESPONSE PROTOCOL

The following protocol is a template only and should be adapted to include the details of relevant personnel that should form part of the response team. The contact details of the response team must be reviewed every six months to ensure they are up to date.

Further guidance about responding to a Privacy Breach is contained in the NCEC/NCISA Privacy Compliance Manual available on the Staff Portal.

Introduction

This protocol sets out the procedure to manage a school's response to the actual or suspected misuse, interference, loss, or unauthorised access, modification or disclosure of personal information (Privacy Breach). It is intended to enable the school to contain, assess and respond to a Privacy Breach.

The School may also wish to seek guidance from Cairns Catholic Education Services.

Response protocol

In the event of a Privacy Breach, School personnel must adhere to the following four phase process (as described in the Office of the Australian Information Commissioner's (OAIC) guide *Data breach notification: a guide to handling personal information security breaches*). Phases 1 – 3 should occur in quick succession and may occur simultaneously.

It is important that appropriate records are kept of the response to the Privacy Breach, including the assessments of the risks associated with the Privacy Breach and decisions made as to the appropriate action/s to take in response to the Privacy Breach.

Phase 1. Contain the Privacy Breach and do a preliminary assessment

1. The school personnel who becomes aware of the Privacy Breach must immediately notify [insert name of appropriate person]. This notification should include (if known at this stage) the time and date the suspected Privacy Breach was discovered, the type of personal information involved, the cause and extent of the Privacy Breach, and who may be affected by the Privacy Breach.
2. [insert name of appropriate person (as per 1)] must take any immediately available steps to contain the Privacy Breach (e.g. contact the IT department, if practicable, to shut down relevant systems or remove access to the systems).
3. In containing the Privacy Breach, evidence should be preserved that may be valuable in determining the cause of the Privacy Breach. This is particularly relevant if there is a Privacy Breach involving information security.
4. [insert name of appropriate person (as per 1)] must consider if there are any other steps that can be taken immediately to mitigate the harm an individual may suffer from the Privacy Breach.
5. [insert name of appropriate person (as per 1)] must make a preliminary assessment of the risk level of the Privacy Breach. This will involve an analysis of the risks involved. 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 Privacy 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.

6. In the event that [insert name of appropriate person (as per 1)] receives multiple reports of Privacy Breaches of different datasets, this may be part of a related incident. [insert name of appropriate person (as per 1)] must consider upgrading the risk level if this situation arises.
7. Where a **High Risk** incident is identified, [insert name of appropriate person (as per 1)] must consider if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals.
8. [insert name of appropriate person (as per 1)] must escalate **High Risk** and **Medium Risk** Privacy Breaches to the response team (whose details are set out at the end of this protocol).
9. If [insert name of appropriate person (as per 1)] believes a **Low Risk** Privacy Breach has occurred, he or she may determine that the response team does not need to be convened. In this case, he or she must undertake Phases 2 and 3 below.
10. If there could be media or stakeholder attention as a result of the Privacy Breach, it must be escalated to the response team.
11. If appropriate, the response team should pre-empt media interest by developing a communications or media response and strategy that manages public expectations.

Phase 2. Evaluate the risks associated with the Privacy Breach

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Privacy Breach and mitigate harm to affected individuals.
2. The response team is to work to evaluate the risks associated with the Privacy Breach by:
    a. identifying the type of personal information involved in the Privacy Breach;
    b. identifying the date, time, duration, and location of the Privacy Breach;
    c. establishing the extent of the Privacy Breach (number of individuals affected);
    d. establishing who the affected, or possibly affected, individuals are;
    e. identifying what is the risk of harm to the individual/s and the extent of the likely harm (e.g. what was the nature of the personal information involved);
    f. establishing what the likely reoccurrence of the Privacy Breach is;
    g. considering whether the Privacy Breach indicates a systemic problem with practices or procedures;
    h. assessing the risk of harm to the school and [AIS/CEC]; and
    i. establishing the *likely* cause of the Privacy Breach.

3. The response team should assess priorities and risks based on what is known.
4. The response team does not need to consider a particular matter above if this will cause significant delay in proceeding to Phase 3.
5. The response team should regularly update each other and other relevant stakeholders regarding incident status.

Phase 3. Consider Privacy Breach notifications

6. Where appropriate, having regard to the seriousness of the Privacy Breach (based on the evaluation above), the response team must determine whether to notify the following stakeholders of the Privacy Breach:
    a. affected individuals;
    b. parents;
    c. the OAIC; and/or
    d. other stakeholders (e.g. if information which has been modified without authorisation is disclosed to another entity, that entity may need to be notified).
7. In general, if a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals (and their parents if the affected individuals are pupils) and the OAIC should be notified.
8. The response team will facilitate ongoing discussion with the OAIC as required.
9. For further information, see section the NCEC/NCISA Privacy Compliance Manual found on the Staff Portal.

Phase 4. Take action to prevent future Privacy 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. The cause of the Privacy Breach must be fully investigated.
11. [insert name of relevant person] must enter details of the Privacy Breach and response taken into a Privacy Breach log. [insert name of relevant person] must, every year, review the Privacy Breach log to identify any reoccurring Privacy Breaches.
12. [insert name of relevant person] must conduct a post-breach review to assess the effectiveness of the school's response to the Privacy Breach and the effectiveness of the Privacy 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 Privacy 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 Privacy Breach and conduct an audit to ensure the plan is implemented.

Useful References

- OAIC's *Data breach notification: a guide to handling personal information security breaches*
- OAIC's *Guide to developing a data breach response plan*
- OAIC's website at www.oaic.gov.au

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.]

Role	Responsibilities and authorities	First contact person	Second contact person
e.g. Project Manager			

Useful contacts

National Computer Emergency Response Team (CERT)
Report Privacy Breaches to CERT via email (info@cert.gov.au) or telephone (1300 172 499).

Office of the Australian Information Commissioner (OAIC)
Report Privacy Breaches to OAIC via email (enquires@oaic.gov.au) or telephone (1300 363 992).

Attachment 5

USE AND DISCLOSURE TABLE

The following Table provides a sequential assessment to guide decisions on authorising the release of information: