CARNARVON
CHRISTIAN SCHOOL
"Walk as Children of Light"

CARNARVON CHRISTIAN SCHOOL - PRIVACY POLICY

30 Babbage Island Road [Po Box 141] Carnarvon 6701 Western Australia
Phone: 08 9941 4533 Fax: 08 9941 4633 Email: office@ccs.wa.edu.au

Contents

1. Scope

This policy applies to members of school staff and the school board at Carnarvon Christian School. This policy will be made available on request.

2. AUTHORISATION

This policy was adopted at the Carnarvon Christian School Board meeting on 31st July 2012.

3. REVIEW DATE

This policy shall be reviewed at the end of February 2020 and updated if required.

4. BACKGROUND

All staff of Carnarvon Christian School are required by law to protect the personal and health information the School collects and holds.

The privacy laws do not replace any existing obligations Carnarvon Christian School has under other laws. Essentially this policy will apply when other laws do not regulate the use of personal information.

5. DEFINITIONS

Personal information means information or opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can be reasonably be determined from the information or opinion. For example this includes all paper and electronic records, photographs and video recordings.

Health information is defined as including information or opinion about a person's physical, mental or psychological health, or disability, which is also classified as personal information. This includes information or opinion about a person's health status and medical history, whether recorded or not.

Sensitive information is defined as information relating to a person's racial or ethnic origin, political opinions, religion, trade union, or other professional, or trade association membership, sexual preferences, or criminal record that is also classified as personal information about an individual.

In this policy *personal information* refers to personal information, health information and

sensitive information unless otherwise specified.

Parent in this policy in relation to a child, includes step parent, an adoptive parent, a foster parent, guardian, or a person who has custody or daily care and control of the child.

Staff in this policy is defined as someone who carries out a duty on behalf of the School, paid or unpaid, or who is contracted to, or directly employed by the School or the Department of Education and Training (DE&T). Information provided to a School through job applications is also considered staff information.

6. Privacy Policy Carnarvon Christian School

(Refer to Principle 5 – People working with children and young people are suitable and supported to reflect child safety and wellbeing values in practice.)

This Privacy Policy sets out how Carnarvon Christian School (CCS) manages personal information provided to or collected by it.

CCS is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988*. In relation to health records, CCS is also bound by the ***Freedom of Information Act 1992***. CCS 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.

7. What kinds of personal information does Carnarvon Christian School collect and how do we collect it?

The type of information CCS 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:
    - 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:
  - 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;

8. What kinds of personal information does Carnarvon Christian School collect and how do we collect it?

- 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 Carnarvon Christian School, including name and contact details and any other information necessary for the particular contact with CCS.

Personal Information you provide: Carnarvon Christian 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 CCS 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.

9. How will Carnarvon Christian School use the personal information you provide?

CCS 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, Carnarvon Christian School's primary purpose of collection is to enable CCS 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 Carnarvon Christian 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 Carnarvon Christian 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 CCS;
- looking after pupils' educational, social and medical wellbeing;
- seeking donations and marketing for CCS; and
- To satisfy Carnarvon Christian School's legal obligations and allow CCS to discharge its duty of care.

In some cases where Carnarvon Christian School requests personal information about a pupil or Parent, if the information requested is not provided, CCS 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, Carnarvon Christian School's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor, as the case may be.

10. How will Carnarvon Christian School use the personal information you provide?

The purposes for which Carnarvon Christian 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 Carnarvon Christian School's legal obligations, for example, in relation to child protection legislation.

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

Marketing and fundraising: Carnarvon Christian School treats marketing and seeking donations for the future growth and development of the school as an important part of ensuring that CCS continues to provide a quality learning environment in which both pupils and staff thrive. Personal information held by CCS may be disclosed to organisations that assist in the School's fundraising, for example, the School's Foundation [or, on occasions, external fundraising organizations].

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

11. Who might Carnarvon Christian School disclose personal information to and store your information with?

Carnarvon Christian 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 CCS, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
- providers of specialist advisory services and assistance to CCS, 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);

12. Who might Carnarvon Christian School disclose personal information to and store your information with?

- people providing administrative and financial services to CCS;
- recipients of CCS publications, such as newsletters and magazines;
- pupils' parents or guardians;
- anyone you authorise CCS to disclose information to; and
- Anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

13 . SECURITY

Sending and storing information overseas: Carnarvon Christian School may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, CCS 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.

Carnarvon Christian 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. CCS personnel and the AISWA 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.

The Carnarvon Christian School currently has an in-house server which is also backed up on-site.

13.1 How does Carnarvon Christian School treat sensitive information?

In referring to 'sensitive information', CCS 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.

13.2 Management and security of personal information

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

CCS 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.

14. 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 CCS 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 Carnarvon Christian School holds about you or your child, please contact the School Principal (Mr. James Shaw) by telephone or in writing. CCS may require you to verify your identity and specify what information you require. CCS 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, CCS 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

15. Consent and rights of access to the personal information of pupils

Carnarvon Christian School respects every Parent's right to make decisions concerning their child's education.

Generally, CCS will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's Parents. CCS 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 our school about them or their child by contacting the School Principal (Mr. James Shaw) 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.

Carnarvon Christian 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.

16. Enquiries and complaints

If you would like further information about the way Carnarvon Christian School manages the personal information it holds, or wish to complain that you believe that CCS has breached the Australian Privacy Principles please contact the School Principal (Mr. James Shaw) by email james.shaw@ccs.wa.edu.au or telephone 99414533. Carnarvon Christian 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.

ANNEXURE 2 PERSONAL INFORMATION TEMPLATE – PARENT

Summary of Personal info (PI) collected	Needed for a function/activity at school	From whom is the PI collected	Where is the PI recorded	Who can access PI	How long Kept?	Level of security risk?	Disclosed outside school?
Key	Y/N	P/A = PARENT P/U = PUPIL SM = Staff member HP = health provider OR = Other(specify)	P=paper file E=electronic file D= database	PR=Principal LS=limited staff AS=all staff OR=other (specify)	A=while pupil enrolled B=up to 6 yrs C=up to 10yrs D=up to 23 yrs from date of incident E=indefinite	H=high M=medium L=low	Y/N
Name							
Address							
Phone number							
Date of Birth							
Birth certificate							
religion							
Parish information							
Conduct reports							
Next of kin							
Emergency contact numbers							
Names of doctors							
School reports							
assessments							
referrals							
Details of disability							
Court orders							
Counselling reports							
Complaint records							
Communication with parents/carers							
Behaviour notes							
Previous school							
Medicare number							
Medical reports							
File notes							
Diary entries							
Case management							
Volunteer info							
Employment info							
Legal case files							
Unsolicited info							

ANNEXURE 1 PERSONAL INFORMATION TEMPLATE – STUDENT

Summary of Personal info (PI) collected	Needed for a function/activity at school	From whom is the PI collected	Where is the PI recorded	Who can access PI	How long Kept?	Level of security risk?	Disclosed outside school?
Key	Y/N	P/A = PARENT P/U = PUPIL SM = Staff member HP = health provider OR = Other(specify)	P=paper file E=electronic file D= database	PR=Principal LS=limited staff AS=all staff OR=other (specify)	A=while pupil enrolled B=up to 6 yrs C=up to 10yrs D=up to 23 yrs from date of incident E=indefinite	H=high M=medium L=low	Y/N
Name							
Address							
Phone number							
Date of Birth							
Birth certificate							
religion							
Parish information							
Conduct reports							
Next of kin							
Emergency contact numbers							
Names of doctors							
School reports							
assessments							
referrals							
Details of disability							
Court orders							
Counselling reports							
Complaint records							
Communication with parents/carers							
Behaviour notes							
Previous school							
Medicare number							
Medical reports							
File notes							
Absence notes							
Case management							
Photos video							
Employment info							
Legal case files							

ANNEXURE 3 PERSONAL INFORMATION TEMPLATE – EMPLOYEE

Summary of Personal info (PI) collected	Needed for a function/activity at school	From whom is the PI collected	Where is the PI recorded	Who can access PI	How long Kept?	Level of security risk?	Disclosed outside school?
Key	Y/N	P/A = PARENT P/U = PUPIL SM = Staff member HP = health provider OR = Other(specify)	P=paper file E=electronic file D= database	PR=Principal LS=limited staff AS=all staff OR=other (specify)	A=while pupil enrolled B=up to 6 yrs C=up to 10yrs D=up to 23 yrs from date of incident E=indefinite	H=high M=medium L=low	Y/N
Name							
Address							
Phone number							
Date of Birth							
Birth certificate							
religion							
Parish information							
Next of kin							
Emergency contact numbers							
Names of doctors							
Job applications							
Profession develop							
Referee contacts							
Appraisal info							
Bank details							
Pay advice							
Complaint records							
Communication with parents/carers							
Role description							
Leave details							
Medicare number							
Medical certificates							
Employment File notes							
Diary entries							
Case management							
Photos videos							
Employment info							
Workplace surveillance							
Workplace emails							

ANNEXURE 4 – DISCLOSURE STATEMENT TO STUDENTS

Counselling at Carnarvon Christian 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

CARNARVON CHRISTIAN SCHOOL
"Walk as Children of Light"

PHOTOGRAPH/VIDEO USAGE FORM

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 Carnarvon Christian School 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 to 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 put a line through "with 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 understand and agree that if I wish to withdraw any consent provided above, it is my responsibility to notify the school.

Children's full names and ages won't be published. We will *not* include in any publications pictures of children in swim suits or pictures which could at all be misconstrued. *Any personal information will be stored, used and disclosed in accordance with the requirements of the* Privacy Act 1988 *(Cth).*

Name of Parent / Guardian (please circle) _____

Signed: Parent/Guardian_____ Date:_____

Yours sincerely
James Shaw
Principal

ANNEXURE 6 – MANDATORY NOTIFICATION OF ELIGIBLE DATA BREACHES SUMMARY

Maintain information governance and security – APP 1 and 11

Schools have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known Data Breach

Contain

C**ontain** a suspected or known Data Breach where possible.

Assess

Schools will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the School has reasonable grounds to believe this is the case, then this is an **EDB** and it must notify individuals affected and the Information Commissioner. If it only has grounds to suspect that this is the case, then it must conduct an **assessment**. As part of the assessment, Schools should consider whether **remedial action** is possible.

Schools should consider adopting the OAIC's suggested a three-stage process:

Initiate: plan the assessment and assign a response team or person

Investigate: gather relevant information about the incident to determine what has occurred

Evaluate: make an evidence-based decision about whether serious harm is likely (and document this).

Schools should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, a School should take steps to reduce any potential harm to individuals. For example, this might involve taking action to recover lost information before it is accessed or changing access controls on accounts before unauthorised transactions can occur. If remedial action is successful in making serious harm no longer likely, then notification is not required and Schools can progress to the review stage.

NO Is serious harm still likely? YES

Notify

Where **serious harm is likely**, a School must prepare a statement for the Commissioner (a form available on OAIC website) that contains:

- the School's identity and contact details
- a description of the Data Breach
- the kind/s of information concerned
- recommended steps for individuals affected

Schools must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the School's website and publicise it

Schools can provide further information in their notification, such as an apology and an explanation of what they are doing about the Data Breach. **In some limited circumstances, an exception to the obligation to notify the individuals or the Commissioner may apply.**

Review

Review the incident and take action to Prevent future Data Breaches. This may include:

- Fully investigating the cause of the Data Breach
- Developing a prevention plan
- Conducting audits
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Schools should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- other external or third parties (eg the ATO)
- The Australian Cyber Security Centre and related agencies
- professional bodies
- Credit card companies or financial services providers

Schools that operate outside Australia may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

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).

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 information	For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself?
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.

Assess the risk of harm to the affected individuals	
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 soughtif 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 harmis 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 mustbe 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.]

DOCUMENT CONTROL

VERSION	DATE PUBLISHED	CHANGES MADE	AUTHOR OF CHANGES
1	30th March 2005	Document drafted	Board
2	2010	Document updated	board
3	July 2012	Document updated	Board
4	Sept 2014	Document updated	Board
5	February 2019	Document updated	Board
6	December 2019	Implement Document control register	Toni Radcliffe
7	December 2019	Reference to National Principles for Child Safe Organisations – pg 3 Table of contents - fixed	James Shaw