Gulf Christian College

Creating Opportunity

Policy No. 11

PRIVACY POLICY

Policy adopted from Nambour Christian College 2011					
ISSUED:NCC	October 2003				
REVISED:	29 July 08	26 July 11	25 March 14	13 Sept 2016	15 May 2018
REVISED:	15 Dec 2021	16 July 2025			

Privacy Policy

Purpose:	The Gulf Christian College is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act. This statement outlines the privacy policy of the school and describes how the school uses and manages personal information provided to or collected by it.	
Scope:	The policy applies to board directors, employers, employees, volunteers, parents/guardians and students, contractors and people visiting the school site; and describes the type of information the school collects, how the information is handled, how and to whom the information is disclosed, and how the information may be accessed.	
References:	• Australian Privacy Principles • Privacy Act 1988 (Cth) • Child Protection Policy • Disabilities Policy	
Supersedes:	Previous GCC Privacy Policy dated 15 December 2021	
Authorised by:	GCC Governing Body	Date of Authorisation: 16 July 2025
Review Date:	Annually, as appropriate, to take account of new laws and technology, changes to school's operations and practices and to make sure it remains appropriate to the changing environment.	Next Review Date: 16 July 2026, or as required
Policy Owner:	GCC Governing Body	

Exception in Relation to Employee Records:

Under the *Privacy Act 1988* (Cth) (Privacy Act), the Australian Privacy Principles do not apply to an employee record held by the employing entity. As a result, this Privacy Policy does not apply to Gulf Christian College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between Gulf Christian College and employee.

Policy

This Privacy Policy sets out how Gulf Christian College manages personal information provided to or collected by it. Gulf Christian College is bound by the Australian Privacy Principles contained in the *Privacy Act.* Gulf Christian College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to Gulf Christian College's operations and practices and to make sure it remains appropriate to the changing school environment.

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

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

- students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the School:
    - 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:
    - 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
- 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:

Gulf Christian College will generally collect personal information held about an individual by way of forms filled out by parents or students, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than parents and students provide personal information.

Personal Information provided by other people:

In some circumstances Gulf Christian College 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.

How will the School use the personal information you provide?

Gulf Christian College 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.

Students and Parents

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

The purposes for which Gulf Christian College uses personal information of students 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 Gulf Christian College
- looking after student's educational, social and medical wellbeing
- seeking donations and marketing for Gulf Christian College
- to satisfy Gulf Christian College's legal obligations and allow the school to discharge its duty of care.

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

On occasions information such as academic and sporting achievements, student activities and similar news is published in School newsletters and magazines, on our intranet and on our website, this may

include photographs and videos of student activities such as sporting events, school camps and school excursions. The School will obtain permissions [annually] from the student's parent or guardian (and from the student if appropriate) if we would like to include such photographs or videos [or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet.

Job applicants, Staff Members and Contractors

In relation to personal information of job applicants, staff members and contractors, Gulf Christian College's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

The purposes for which Gulf Christian College uses personal information of job applicants, staff members and contractors include:

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

Volunteers

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

Marketing and Fundraising

Gulf Christian College treats marketing and seeking donations for the future growth and development of the school as an important part of ensuring that Gulf Christian College continues to provide a quality learning environment in which both students and staff thrive. Personal information held by Gulf Christian College may be disclosed to organisations that assist in the school's fundraising, for example, the Gulf Christian College'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.

If you would like to opt-out of direct marketing please contact College Business Office on business@gulfcc.qld.edu.au or telephone the office on 07 4745 1180.

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

Gulf Christian College may disclose personal information, including sensitive information, held about an individual for educational, legal, administrative, marketing and support purposes. This may include to:

- another school or staff at another school
- government departments (including for policy and funding purposes)
- medical practitioners
- people providing educational, support and health services to the School, including specialist visiting teachers, [sports] coaches, volunteers, counsellors and providers of learning and assessment tools
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN)
- people providing administrative and financial services to Gulf Christian College;
- recipients of School publications, such as newsletters and magazines
- students' parents or guardians
- anyone you authorise Gulf Christian College to disclose information to
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Sending and Storing Information Overseas

Gulf Christian College may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, Gulf Christian College 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)
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

Gulf Christian College may use online or 'cloud' service providers to store personal information and to provide services to Gulf Christian College 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 server which may be situated outside Australia.

Sensitive Information

In referring to 'sensitive information', Gulf Christian College 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 required by law.

Management and Security of Personal Information

Gulf Christian College 's staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals. Gulf Christian College has in place steps to protect the personal information Gulf Christian College 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.

Data Breaches

It will be deemed that an 'eligible data breach' has occurred if:

- there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals (the affected individuals)
- a reasonable person would conclude there is a likelihood of serious harm to any affected individuals as a result
- the information is lost in circumstances where:
    - unauthorised access to, or unauthorised disclosure of, the information is likely to occur
    - assuming unauthorised access to, or unauthorised disclosure of, the information was to occur, a reasonable person would conclude that it would be likely to result in serious harm to the affected individuals.

Serious harm may include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

What must the school do in the event of an 'eligible data breach'?

If Gulf Christian College suspects that an eligible data breach has occurred, it will carry out a reasonable and expedient assessment/investigation within 30 days.

If such an assessment/investigation indicates there are reasonable grounds to believe an eligible data breach has occurred, then Gulf Christian College will be required to lodge a statement to the Privacy Commissioner (Commissioner). Where practical to do so, the school entity will also notify the affected individuals. If it is not practicable to notify the affected individuals, Gulf Christian College will publish a copy of the statement on its website, or publicise it in another manner.

Exception to notification obligation

An exception to the requirement to notify will exist if there is a data breach and immediate remedial action is taken, and as a result of that action:

- there is no unauthorised access to, or unauthorised disclosure of, the information
- there is no serious harm to affected individuals, and as a result of the remedial action, a reasonable person would conclude the breach is not likely to result in serious harm.

Access and Correction of Personal Information

Under the *Privacy Act*, an individual has the right to seek and obtain access to any personal information which Gulf Christian College holds about them and to advise Gulf Christian College of any

perceived inaccuracy. There are some exceptions to this right set out in the Act. Students will generally be able to access and update their personal information through their parents, but older students may seek access and correction themselves.

To make a request to access or to update any personal information Gulf Christian College holds about you or your child, please contact the College Principal in writing. Gulf Christian College may require you to verify your identity and specify what information you require. Gulf Christian College 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, Gulf Christian College 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.

The School will take reasonable steps to ensure that any personal information is accurate, up to date, complete, relevant and not misleading.

Consent and Rights of Access to the Personal Information of Students

Gulf Christian College respects every parent's right to make decisions concerning their child's education. Generally, Gulf Christian College will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. Gulf Christian College will treat consent given by parents as consent given on behalf of the student and notice to parents will act as notice given to the student.

As mentioned above, parents may seek access to personal information held by Gulf Christian College about them or their child by contacting the College Principal. However, there will 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 Gulf Christian College 's duty of care to a student.

The School may, at its discretion, on the request of a student grant that student access to information held by Gulf Christian College about them, or allow a student to give or withhold consent to the use of their personal information, independently of their parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Enquiries and Complaints

If you would like further information about the way Gulf Christian College manages the personal information it holds, or wish to make a complaint about Gulf Christian College's breach of the Australian Privacy Principles please contact the College Principal on email principal@gulfcc.qld.edu.au or phone 07 4745 1180. Gulf Christian College 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.

Definitions

Australian Privacy Principles (at Oct 2020)

https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/

1. *Open and transparent management of personal information*

2. *Anonymity and pseudonymity*
3. *Collection of solicited personal information*
4. *Dealing with unsolicited personal information*
5. *Notification of the collection of personal information*
6. *Use or disclosure of personal information*
7. *Direct marketing*
8. *Cross-border disclosure of personal information*
9. *Adoption, use or disclosure of government related identifiers*
10. *Quality of personal information*
11. *Security of personal information*
12. *Access to personal information*
13. *Correction of personal information*

Breach means unauthorized access and unauthorized disclosure of personal information of individuals including in circumstances where there has been a possible unauthorized access or disclosure which compromises personal data.

Eligible data refers to personal information of a sensitive (confidential) nature which could result in significant harm / damage or risk to those affected by a breach.

Examples of eligible data breaches include:

- Disclosures of Medicare numbers or financial accounts; and
- Disclosure of mental illness, disability, or residential address of "protected people".

The consequences of eligible data breaches can include:

- Threat to emotional wellbeing;
- Damage to reputation; and
- Defamation

Employee means all employees employed by the College, including applicants and prospective employees.

Employee Record means a record as defined by the Act. (Employment Records are exempt from Privacy Protection)

Health information is a subset of sensitive information. It is information or an opinion about the health or disability of an individual and information collected to provide, or in providing a health service.

Health Service includes an activity performed to assess, record, maintain or improve an individual's health, to diagnose an illness or disability, to treat an individual, or the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Mandatory Notification means that the College must notify the Australian Information Commissioner when an eligible breach has occurred.

Parent is the parent / guardian / carer of a student.

Personal Information is information or an opinion, whether true or not and whether recorded in material form or not, about an identified individual or an individual whose identity is reasonably apparent, or can be determined, from the relevant information or opinion.

Response Plan means the Plan followed by the Response team following an actual or suspected breach of data.

Response Team is a small group of delegated staff whose role is to respond to alleged or known breaches of personal information held by the College.

Sensitive information is a type of personal information. It includes information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practice, or criminal record. Sensitive information also includes biometric information that is used for the purpose of automated biometric verification, biometric identification or biometric templates.

Student means prospective, current, or past student of the College.

Appendices Attached:

- Appendix 1: Standard Collection Notice
- Appendix 2: Alumni Collection Notice
- Appendix 3: Employment Collection Notice
- Appendix 4: Contractor / Volunteer Collection Notice
- Appendix 5: Notification Statement to the Office of the Information Commissioner (OAIC) 2018
- Appendix 6: Privacy Breach Checklist
- Appendix 7: Privacy Breach Response Plan

APPENDIX 1

Standard Collection Notice

1 The School collects personal information, including sensitive information about students and parents or guardians before and during the course of a student'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 students enrolled at the school, exercise its duty of care, engage in marketing/fundraising and perform necessary associated administrative activities, which will enable students 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 students 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 students from time to time.
5. The School may disclose personal and sensitive information for educational, legal, administrative, marketing and support purposes. This may include to:
   - other schools and teachers at those schools;
   - government departments (including for policy and funding purposes);
   - medical practitioners;
   - people providing educational, support and health services to the School, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
   - providers of learning and assessment tools;
   - assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
   - people providing administrative and financial services to the School;
   - anyone you authorise the School to disclose information to; and
   - anyone to whom the School is required or authorised by law, including child protection laws, to disclose the information.
6. Personal information collected from students is regularly disclosed to their parents or guardians.
7. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of on online or 'cloud' service providers is contained in the School's Privacy Policy.**
8. The School's Privacy Policy, accessible on the School's website, sets out how parents or students 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 a student, or where students have provided information in confidence. Any refusal will be notified in writing with reasons if appropriate.

9. The School's Privacy Policy also sets out how parents and students 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, student activities and similar news is published in School newsletters and magazines, on our intranet and on our website, this may include photographs and videos of student activities such as sporting events, school camps and school excursions. The School will obtain permissions [annually] from the student's parent or guardian (and from the student if appropriate) if we would like to include such photographs or videos [or other identifying material] in our promotional material or otherwise make this material available to the public such as on the internet.
12. We may include students' and students' parents' contact details in a class list and School directory. †
13. If you provide the School with the personal information of others, such as doctors or emergency contacts, we encourage you to inform them that you are disclosing that information to the School and why.

***** As appropriate

****** If applicable

† Schools may wish to seek specific consent to publish contact details in class lists and School directories

APPENDIX 2

Alumni Collection Notice

1. We may collect personal information about you from time to time. The primary purpose of collecting this information is to enable us to inform you about our activities and the activities of Gulf Christian College and to keep alumni members informed about other members.
2. We must have the information referred to above to enable us to continue your membership of the Gulf Christian College Alumni.
3. As you know, from time to time we engage in fundraising activities. The information received from you may be used to make an appeal to you. It may also be used by Gulf Christian College to assist in its fundraising activities. If you do not agree to this, please advise us now.
4. We may publish details about you in our newsletter and our School's website. If you do not agree to this, you must advise us now.
5. The School's Privacy Policy, accessible on the School's website, contains details of how you may seek access to and correction of your personal information which the School has collected and holds, and how you may complain about a breach of the Australian Privacy Principles.
6. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as email services. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of on online or 'cloud' service providers is contained in the School's Privacy Policy. *
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

* If applicable

APPENDIX 3

Employment Collection Notice

1. In applying for this position, you will be providing Gulf Christian College with personal information. We can be contacted by mail at PO Box 210, Normanton Qld 4890 or by email at business@gulfcc.qld.edu.au or by telephone on 07 4745 1180.
2. If you provide us with personal information, for example, your name and address or information contained on your resume, we will collect the information in order to assess your application for employment. We may keep this information on file if your application is unsuccessful in case another position becomes available.
3. The School's Privacy Policy, accessible on the School's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your personal information which the School has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others. Any refusal will be notified in writing with reasons if appropriate.
4. We will not disclose this information to a third party without your consent unless otherwise permitted.
5. We are required to conduct a criminal record check/Working with Children check to collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection laws*. We may also collect personal information about you in accordance with these laws. *
6. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as email services. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of on online or 'cloud' service providers is contained in the School's Privacy Policy. *
7. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

* If applicable

APPENDIX 4

Contractor/Volunteer Collection Notice

1. In offering, applying or agreeing to provide services to the School, you will be providing Gulf Christian College with personal information. We can be contacted by mail at PO Box 210, Normanton Qld 4890 or by email at business@gulfcc.qld.edu.au or by telephone on 07 4745 1180.
2. If you provide us with personal information, for example your name and address or information contained on your resume, we will collect the information in order to assess your application. We may also make notes and prepare a confidential report in respect of your application.
3. You agree that we may store this information for a specified period of time.
4. The School's Privacy Policy, accessible on the School's website, contains details of how you may complain about a breach of the Australian Privacy Principles and how you may seek access to and correction of your personal information which the School has collected and holds. However, access may be refused in certain circumstances such as where access would have an unreasonable impact on the privacy of others. Any refusal will be notified in writing with reasons if appropriate.
5. We will not disclose this information to a third party without your consent unless otherwise permitted to.
6. We are required to conduct a criminal record check/ Working with Children check to collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences under Child Protection law. * We may also collect other personal information about you in accordance with these laws. *
7. The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of on online or 'cloud' service providers is contained in the School's Privacy Policy. *
8. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

***** If applicable

APPENDIX 5

Notification Statement to the Office of the Information Commissioner (OAIC) 2018

Used for Mandatory Reporting to Privacy Commissioner
(Where there is a risk of serious harm to individuals or school arising from Privacy Breach)

Contact details of School: _____

_____

Details of the **Eligible Breach** (significant harm):_____

_____

Nature of possible serious harm: _____

_____

Remedial/mitigation action taken: _____

_____

Who are the likely affected individuals? _____

_____

How many individuals may be affected? _____

_____

Is notification to individuals sufficient or is the College making a public notification via the College website or social media?

_____

Future actions:_____

_____

Date: _____ Email for Commissioner is enquiries@oaic.gov.au

APPENDIX 6

Privacy Breach Checklist

Form: Breach Checklist for Response Team (Evaluation and Mitigation)

(To be used for a preliminary assessment of level of risk (High, Medium or Low) arising from Breach)

Date Breach occurred: _____

Date Breach reported: _____

Date of Completion of Checklist: _____

The Response Team has followed the following steps:

- ☐ identified the type of personal information involved in the Privacy Breach
- ☐ identified the date, time, duration, and location of the Privacy Breach
- ☐ established the extent of the Privacy Breach (number of individuals affected)
- ☐ considered what mitigation actions are appropriate in the long term
- ☐ established who the affected, or possibly affected, individuals are
- ☐ assessed whether there needs to be a 'public' notification using social media (in addition to contacting individuals who are affected);
- ☐ reached a preliminary assessment of breach:
    - ☐ High
    - ☐ Medium
    - ☐ Low
- ☐ proceeded in accordance with the assessment level;
- ☐ entered a record of the Breach Log.

Name: Principal/Delegate for the Response Team: _____

Signature of Principal/Delegate for the Response Team: _____

Date: _____

APPENDIX 7

PRIVACY BREACH RESPONSE PLAN

Response Plan (required by legislative changes to Privacy Law effective from 22 February 2018)

The Australian Information Commissioner advises the importance of keeping **appropriate records** of responses to Privacy Breaches, by way of transparent and consistent use of a **Response Plan.** The Response Plan will include 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.

The Response Plan is a 4-Phase Process.
In the event of a Privacy Breach, College 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).
Phase 1-3 should occur in quick succession and may occur simultaneously.

Phase 1
Contain the Privacy Breach and do a preliminary assessment.
College personnel who become aware of the privacy breach must immediately notify the Principal or delegate who will inform the Response Team.

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.

The Principal/delegate and Response Team **must take immediate 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).

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.

The Principal/delegate and Response Team delegate **must consider** if there are any other steps that can be taken immediately to mitigate the harm any individuals may suffer from the privacy breach.

The Principal/delegate and Response Team delegate must make a **preliminary assessment** of the risk level of the privacy breach. This will involve an analysis of the risks involved:

- High
- Medium
- Low

Where a High-Risk incident is identified, it falls into the category of an eligible breach (mandatory reporting) and it must be treated as such by the Principal (and Response Team).

They **must consider** if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals. The breach must also be reported to the Office of the Australian Information commissioner within 30 days.

If the breach is identifies as **Medium Risk** and is reasonably considered to be an 'eligible' breach (mandatory reporting) a notification must be made to the Commissioner – Annexure Form.

If the breach is considered **Low Risk, Phase 2 and 3 below must be followed.**

Phase 2

Evaluation and Mitigation of the risks associated with the privacy breach (assessed as High, Medium or Low).

The Response Team is required to take **further steps** available (i.e. additional to those identified in Phase 1) to contain the privacy breach and mitigate harm to affected individuals by:

- Identifying the type of personal information involved in the privacy breach
- Identifying the date, time, duration and location of the privacy Breach;
- Establishing the extent of the privacy breach **(number** of **individuals** affected);
- Establishing **who** the affected, or possibly affected, individuals are;
- Assessing whether there needs to be a 'public' notification using social media;
- 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);
- Assessing the risk of harm to the College;
- Establishing what the likely **reoccurrence** of the privacy breach is;
- Considering whether the privacy breach indicates a **systemic problem** with practices or procedures; and
- Establishing the likely cause of the privacy breach.

Phase 3

Privacy Breach Notifications

It is the responsibility of the Response Team to determine whether to notify the following stakeholders of the privacy breach.

- Affected individuals
- Parents
- The Privacy Commissioner, and/or
- Other stakeholders (other entities who may share information).

The main consideration before choosing what action to take is to ask:

'Does this breach raise a **real risk of serious harm** to affected individuals or the College?'

The Response Team

- The response Team is to be chosen to reflect their skills and their authority to take action when there is a breach of privacy.
- All staff must be aware of their responsibility to inform the Team of a breach.
- Each person on the response Team needs to know what action he/she is responsible for when there is a breach.

Role	Responsibilities and Authority for…	First person to contact?	Second person to contact?
Principal			
IT			
HR			
Legal			
Other			

Other			

The **Investigation of the breach** will be guided by:

- The Response Plan; and
- The College Formal Complaints Policy

Phase 4
Action to prevent future privacy breaches

Additional to following the Response Plan and Formal Complaints Policy, details of

- The breach;
- The cause; and
- The outcome

must be recorded in a **Privacy Breach Log.**

The Principal must review the Breach Log annually, to identify any recurring breaches.
All staff is to be trained in privacy principles and awareness of the confidentiality of the copious personal and sensitive information available to them and accessible to them and that breaching privacy is an offence.

Staff in positions of managing copious amounts of personal and sensitive information (Bursars, PA's, IT personnel) must be aware of their special responsibility and that breaching of privacy is now considered an offence which MUST frequently be reported to the Privacy Commissioner.

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 (enquiries@oaic.gov.au) or telephone (1300 363 992).

Date signed_____