

COLLEGE POLICY 15.0

PRIVACY POLICY

ISSUED:	October 2003	LOCATED:	T:\Admin\Executive\1.College Policies - All major College policies\College Policies		
REVISED:	29 July 2008	26 July 2011	October 2012	25 March 14	July 2017 - aligned with GCC 9/16. Still under Review due to continual law changes
	27 February 2018 (updated from ISQ January 2018 policy to include data breach)	Approved at Board 27 October 2020	8/12/2021 COVID vaccination details included in item 12. Approved by GV	Approved at Board 22 February 2022	March 2023 – Aligned with ISQ and approved at Exec. Approved at Board 28 March 2023

1. Introduction

Nambour 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 to or collected by it.

2. Scope

The policy applies to Board members, 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.

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

3. Legislation, documentation & policies

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (<https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/>)
- Application Forms
- Admission/Enrolment Contract
- Child Protection Policies & Procedures
- Policies for students with disabilities
- Other relevant College Policies

4. 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 the College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and employee.

5. What kind of personal information does the College collect and how does the College collect it?

The type of information the College collects and holds includes, but is not limited to, personal information, including sensitive information about:

- Students and parents and/or guardians (herein called 'parents') before, during and after the course of a student's enrolment at the College;
 - 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 (eg 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 (eg 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 College, including name and contact details and any other information necessary for the particular contact with the school

Unsolicited information provided to the College by third parties will be destroyed unless required to be addressed by law.

Personal Information you provide: The 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 the 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 College use the personal information you provide? The 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.

6. Students and Parents

In relation to personal information of students and parents, the College's primary purpose of collection is to enable the 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 the College throughout the whole period the student is enrolled.

The purposes for which the College uses personal information of students and parents includes:

- To keep parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines
- Day to day administration of the College
- Looking after student's educational, social and medical wellbeing
- Seeing donations and marketing for the College
- To satisfy the College's legal obligation and allow the school to discharge its duty of care.

In some cases where the College requests personal information about a student or parent, if the information requested is not provided, the 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 newsletters and magazines and on our website, this may include photographs and videos of student activities such as sporting events, school camps and school excursions. The College 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.

7. Job applicants, Staff members and Contractors

In relation to personal information of job applicants, staff members and contractors, the 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 the 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 College;
- To satisfy the College's legal obligations, for example, in relation to child protection legislation.

8. Volunteers

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

9. Marketing and fundraising

The College treats marketing for the future growth and development of the College as an important part of ensuring that the College continues to be an excellent learning environment in which both students and staff thrive. Personal information held by the College may be disclosed to an organisation that assists in the College's fundraising, for example, the Colleges Foundation or alumni organisation.

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.

10. Who might the College disclose personal information to and store your information with?

The College may disclose personal information, including sensitive information, held about an individual for educational, legal, administrative, marketing and support purposes 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 College, including specialist visiting teachers, sport 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 the College
- Recipients of College publications, such as newsletters and magazines;
- Parents and guardians;
- Anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

11. Sending and storing information overseas

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

- Obtaining the consent of the individual (in some instances this consent will be implied), or
- Otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The College may disclose personal Information to a reputable overseas entity such as a cloud-hosting service provider for the purposes of delivering educational and support services across the College. 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.

Where student use of an airline or cloud-based service requires parental consent, and the College deems the use of the service is appropriate for the provision of educational or administrative services, parental consent is implied by acceptance of this policy (as part of enrolment), instead of a separate signed parental consent for each of these individual services.

12. Sensitive Information?

In referring to 'sensitive information', the College means: information relating to an individual'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.

13. Management and security of personal information

College employees are required to respect the privacy of individuals and respect the confidentiality of students and parents' personal information.

The College has in place reasonable steps to protect the personal information the 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.

14. 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 an event of an 'eligible data breach'?: If the 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 the 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, the 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.

15. 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 the College holds about them and to advise the 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 any information the College holds about you or your child, (if you are unable to update/view the information yourself through the Parent Lounge), please contact the:

- Executive Principal or Head of Business Operations
PO Box 500, Nambour, QLD, 4560
Phone: 5451 3333
Email: info@ncc.qld.edu.au

The College may require you to verify your identity and specify what information you require. The 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, the College will advise the likely cost in advance.

If a request for access is refused, in accordance with the APP, the College will provide written reasons why the request was refused. Details on how to make a complaint will also be included in this response.

The basis upon which access to records can be refused are as follows:

- In the case of personal information other than health information, that providing access would pose a serious and imminent threat to the life or health of any individual;
- In the case of health information, that providing access would pose a serious threat to life or health of any individual;
- Providing access would have an unreasonable impact upon the privacy of other individuals;
- The request for information is frivolous or vexatious;
- The information relates to existing or anticipates legal proceedings between the College and the individual, and the information would not be accessible through the process of discovery in those proceedings;
- Providing access would reveal the College's intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- Providing access would be unlawful;
- Denying access is required or authorised by or under law (such as in relation to legally privileged information);
- Providing access would be likely to prejudice an investigation of possible unlawful activity;
- Providing access would be likely to prejudice;
 - The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - The enforcement of laws relating to the confiscation of the proceeds of crime;
 - The protection of the public revenue;
 - The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - The preparation for or conduct of, proceedings before any court or tribunal, or implementations of its orders.

16. Consent and Rights of Access to the Personal Information of Students

The College respects every parent's right to make decisions concerning their child's education. Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The 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 above, parents may seek access to personal information held by the College about them or their child by contacting the Executive Principal. However, there will be occasions when access is denied. Such occasions would include where release may result in a breach of the College's duty of care to a student.

The College, may at its discretion, on the request of a student grant that student access to information held by the 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.

17. Archived Materials

Personal information is stores in hard copy and electronically. The Australian Privacy Principles do not state any specific time that records are to be archived. They simply provide that a school is not required to store personal information longer than 'necessary for its purposes'.

It is College policy to maintain complete student files and employee records for a reasonable time following their departure from the College. This is done to protect the interest of both the College and the relevant individual in terms of enquiries or allegations that may be made at any time in the future. The College reserves the right to charge a fee for access to non-current enrolments or employment as outlined above.

Hard Copy Tax File Number (TFN) Declarations

Where the College receives completed hard copy TFN Declaration Forms, the Tax File Number must be "blacked out" once the details have been entered into the payroll system. The form should then be placed in the employees Personnel File.

Electronic Tax File Number (TFN) Declarations

Where employees submit their TFN Declaration electronically, the record is contained electronically in the organisations document storage solution. Only authorised employees have access to these files.

18. Archiving and destruction

Unless subject to a relevant Notice, the College is required to keep time and wages records for its employees for seven years. Privacy legislation does not state how long archives of personal information are to be kept. Essential employee records are not destroyed, but held indefinitely.

19. Data Breaches and Mandatory Notification to the Office of the Australian Information Commissioner (OAIC)

A Notifiable Data Breach occurs when personal information of an individual held by the College is accessed by, or is disclosed to, an unauthorised person, or is lost, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual; or in the case of loss (e.g. leaving a laptop containing personal information on a bus).

Unauthorised access or disclosure of personal information is likely to occur, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual.

20. Response Plan/Process for known or alleged breach of privacy

If the College knows or reasonably suspects that a data breach of privacy has occurred,

- It will call together the Response Team.
- The Response Team will activate the 4 Step Response Plan/Process.
- See Annexure D
- The Response Team will conduct a reasonable and expeditious **initial assessment** to determine the nature and extent of the breach and if there are reasonable grounds to believe that a Notifiable Data Breach has occurred;
- It will take all reasonable steps to ensure that a full assessment is completed within 30 days of becoming aware of the suspected Notifiable Data Breach.

21. Notification

Subject to any restriction under the Act, in the event a Notifiable Data Breach occurs, the College will, as soon as practicable, prepare a statement outlining details of the breach, and;

- Notify the individual of the unauthorised access, disclosure or breach; and
- Notify the Office of the Australian Information Commissioner of the unauthorised access, disclosure or breach.
- See Annexure C

22. Enquiries and Complaints

If an individual believes that the College has breached the APP, a complaint can be made to the College.

All complaints should be in writing and directed to the Principal/Privacy Officer. The College will investigate complaints in a timely manner and respond in writing.

If an individual is not satisfied with the College's response, a complaint can be lodged with the Office of the Australian Information Commissioner on <http://www.oaic.gov.au/privacy/making-a-privacy-complaint>

The College also allows individuals to 'opt out' through the selection on the Standard Collection Notice, or on the enrolment agreement.

23. 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.

24. Review

This policy will be updated bi-annually or as necessitated by law.

Annexures A, B, C, and D attached.



Annexure A

Alumni Privacy Collection Notice

1. The school may collect personal information about you for the purpose of providing up to date information about the activities of the Association and its members highlighting, as appropriate, historical events and achievements of the school and its past pupils and to keep the alumni members informed about other members.
2. The information provided ensures continuing and meaningful membership.
3. We also, from time to time engage in fundraising activities. The information received from you may be used by the school to assist in its fundraising activities and may be used to make an appeal to you for donations. If you do not agree to this, please advise us now.

☐ I agree

☐ I do not agree

4. The school may publish details about you in school publications and the College website. If you do not agree to this, please advise us now.

☐ I agree

☐ I do not agree

5. The College Privacy Policy, accessible on the College website, contains details of how you may seek access and update personal information that the College has collected and holds, and how to make a complaint about a breach of the Australian Privacy Principles.
6. The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as email services. Some essential personal information may also be provided to these service providers to enable them to authenticate users that access their services. This stored personal information may be cloud-based and outside of Australia. Further information about the College's use of online or cloud service providers is contained in the College's Privacy Policy.
7. It may be the case that you give the College details of other potential members. If you provide us with personal information of others, we encourage you to inform them that you are disclosing that information to the College and why.

Name of Applicant/Member: _____

Signature: _____ Date: _____



Annexure B

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



Annexure C

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: _____



Annexure D

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 identified 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_____