	GOVERNANCE
POL- 227	PRIVACY POLICY
Owner	Head of School
Date of First Publication	12 March 2014
Related Documents	The Privacy Act 1988 and Australian Privacy Principles (APPs) POL-060 Crises Response Plan POL-229 Confidentiality Policy POL-253 Complaints Policy (Students & Parents) POL-256 Closed Circuit Television Network Policy POL-268 Complaints Policy (Staff)

Version	Date Published	Changes	Author
2	29 May 2018	Reviewed against introduction of new student learning portal SEQTA, Consent2Go for collection of personal, health and sensitive confidential information, and NDB Scheme obligations under Privacy Act, effective 22 February 2018	GMG

This policy outlines how the School complies with the requirements of the Privacy Act and, in particular, the new Privacy Laws and associated Australian Privacy Principles (APPs) that commenced on 12 March 2014.

The Policy has been prepared to comply with Australian Privacy Principle – Privacy Policy, clauses 1.3 and 1.4.

Personal Information is information that identifies an individual, or could identify an individual. A name or address is an obvious example. In some cases, a date of birth and postcode may be enough to identify an individual. Personal information can also include medical records, bank account details, photographs, videos, and information about where the individual works.

WHAT KINDS OF PERSONAL INFORMATION DOES THE SCHOOL COLLECT AND HOLD (APP 3 & 4)

The type of personal information, including sensitive information, that the School collects and holds, is that which is necessary or directly related to the School's primary function of providing an education and associated activities, or in certain circumstances, a secondary associated function.

For future students and their parents this includes names, contact details and current or previous schooling records.

For current students this includes demographic information, parent/guardian names and contact details, medical information (including, but not limited to immunisation records, disabilities, allergies and absence notes), emergency contacts, current or previous schooling records, and any other information required for the educational, pastoral and health care of the child whilst at the School.

For former students and families this includes name, address and contact details, and other information that may be provided unsolicited by the individual such as change of marital status or occupation.

For parents/guardians this includes names and contact details, occupation and educational qualifications as required by the Federal Government to meet accountability requirements and to qualify for Federal Government funding for the School. It may also include bank account details for School Fee payment if the parent provides this as a preferred payment option.

For staff members this includes names, address, contact details for themselves and spouse (emergency), mandatory registrations, medical information if necessary for personal health and safety, tax file numbers and bank account details, salary, superannuation and leave details, complaint records and investigation reports, photographic material, CCTV information, email and internet browsing history.

For volunteers and contractors this includes names, contact and company details, mandatory registrations and, in some instances, bank account details.

There will individuals who will visit the School periodically, from whom it will be necessary to collect personal information, and this would include names, contact details, and mandatory registrations as required.

HOW THE SCHOOL COLLECTS PERSONAL INFORMATION (APP 5)

The School will generally collect personal information held about an individual by way of forms filled out by parents or students, staff members, job applicants and others, or by face-to-face meetings and interviews, telephone calls, email communications, the School's website and portal, third party service providers (Consent2Go).

In some circumstances the School may be provided with personal information about an individual from a third party, for example a report provided by a medical professional, Government Agency, or a reference from another school.

HOW THE SCHOOL TREATS SENSITIVE INFORMATION

In referring to 'sensitive information', the School means, information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices, or criminal record, that is also personal information; and health 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 the individual agrees otherwise, or the use or disclosure of the sensitive information is allowed by law.

MANAGEMENT AND SECURITY OF PERSONAL INFORMATION (APP 1)

The School's staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals.

The School holds personal information provided by individuals in one, or both, of two formats. The first is the format in which the information was provided, whether this be via a School form, an email, letter, school website/portal communication or a recorded phone message. The second format is within the School's electronic data information management system, Synergetic and the student learning portal, SEQTA.

Hard copies of personal information are held on student or staff personal or medical files, or files created for specific information management purposes such as camp files, or Working with Children Check files. These are secured in filing cabinets, within offices that are locked each night or in controlled access areas.

Access to personal information entered into Synergetic and SEQTA is controlled by password access and security levels assigned to each staff member. The level of access for each staff member is determined by their role within the School and their operational requirement to know specific personal information about an individual.

THE PURPOSE FOR WHICH THE SCHOOL COLLECTS, HOLDS, USES AND DISCLOSES PERSONAL INFORMATION (APP 6, 7 & 8)

The School will use the personal information it collects for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or for which the individual has consented.

Students and Parents/Guardians

In relation to personal information of students and parents/guardians, the School's primary purpose of collection is to enable the School to provide schooling for the student enrolled at the School. This includes satisfying both the needs of parents/guardians and the needs of the student throughout the whole period the student is enrolled at the School.

The purposes for which the School uses personal information of students and parents/guardians include:

- to keep parents/guardians informed about matters related to their child's schooling, through correspondence, newsletters, magazines and the School's website;
- day-to-day administration;
- looking after students' educational, social and medical wellbeing;
- seeking donations and marketing for the School;
- to satisfy the School's legal and legislative obligations and allow the School to discharge its duty of care.

In some cases, where the School requests personal information about a student or parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the student, or permit the student to participate in a particular activity.

Job applicants, staff members, and contractors

In relation to personal information of job applicants, staff members and contractors, the School'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 School uses personal information of job applicants, staff members, and contractors include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the School;
- 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 the School in its functions or to conduct associated activities (such as the Old Grammarians' Association - OGA), to enable the School and the volunteers to work together.

Marketing and fundraising
The School treats marketing and seeking donations for the future growth and development of the School, as an important part of ensuring that the School continues to provide a quality-learning environment in which both students and staff thrive. Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising, for example, the School's Foundation or the OGA or the Parents & Friends' Association (P&F).

The School provides the opportunity for individuals to deny the disclosure of their personal information to the P&F within the Confidential Personal Information form.

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

TO WHOM MIGHT THE SCHOOL DISCLOSE PERSONAL INFORMATION (APP 6)
The School may disclose personal information, including sensitive information, held about an individual to:

- another school for student transfers;
- in order to facilitate school exchanges or Round Square exchanges, the School may disclose personal information about a student to an overseas recipient; the individual's consent will be sought before so doing;
- State and Federal government departments directly associated with educational services or school grant funding;
- medical practitioners, people providing services to the School, including specialist visiting teachers, school camp providers such as Outward Bound, sports coaches and volunteers;
- assessment and educational authorities, including Australian Curriculum Assessment and Reporting Authority (ACARA), NAPLAN Test Administration Authorities;
- recipients of School publications, like newsletters and magazines;
- Parents/Guardians;
- anyone the individual or parent/guardian authorises the School to disclose information to; and
- anyone to whom the School is required or authorised to disclose information to be law, including child protection laws.

HOW TO ACCESS AND CORRECT PERSONAL INFORMATION (APP 12 &13)
Under the Commonwealth Privacy Act and Australian Privacy Principles 12 & 13, an individual has the right to obtain access to any personal information, which the School holds, about them and to advise the School of any perceived inaccuracy. There are a number of exceptions to this right, as set out in Australian Privacy Principle 12, clause 12.3. Such exceptions 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 student.

Parents may seek access to personal information held by the School about them or their child by contacting the Head of School in writing. Students will generally have access to their personal information through their parents, but older students may seek access themselves. The School may, at its discretion, on the request of a student, grant that student access to information held by the School 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 so warranted.

The School may require the individual to verify their identity and specify what information they require. The School may charge a fee to cover the cost of verifying the application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Staff, past students, volunteers, and contractors may seek access to their personal information by contacting the Bursar or Head of School in writing. Job applicants may seek access to their personal information by contacting the Human Resources Officer.

The School is required to respond to a request for access to personal information within 30 days of the request or within a reasonable period after the request is made.

The School may refuse, under certain circumstances, to give access to personal information as requested or to give access in the manner requested by the individual or, their parent/guardian if the individual is a student. If this occurs, the School must give the individual a written notice that states the reason for the refusal and the mechanisms available to the individual to complain about the refusal and any other related matter prescribed by the regulations.

CORRECTION OF PERSONAL INFORMATION (APP13)

If under Australian Privacy Principle 13 – Correction of personal information, the School believes that the personal information held is inaccurate, out-of-date, incomplete, irrelevant, or misleading or the individual requests the School to correct the information, the School must take such steps as reasonable in the circumstances to correct the information.

The School endeavours to ensure that the personal information it holds is accurate, complete, up-to-date, and relevant. The School annually requests that individuals confirm or update critical personal information for current students and families via the BCGS Confidential Personal Information Form. In addition, a person may seek to update their personal information held by the School, at any time, by contacting the Administration Office of the School or via the School's parent portal.

Staff and job applicants can contact the Human Resources Officer and contractors can contact the School Bursar or Assistant Bursar.

The School is required to respond to a request to correct personal information within 30 days of the request or within a reasonable period after the request is made.

The School may refuse, under certain circumstances, to correct personal information as requested by the individual or, their parent/guardian if the individual is a student. If this occurs, the School must give the individual a written notice that states the reason for the refusal and the mechanisms available to the individual to complain about the refusal and any other related matter prescribed by the regulations.

DISCLOSURE OF PERSONAL INFORMATION TO OVERSEAS RECIPIENTS (APP 8)

Many students travel overseas on Round Square exchanges, conferences, and service trips for which it is necessary to provide certain personal information. The School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principle 8 – Cross border disclosure of personal information.

APP 8 requires the School to take such steps as are reasonable in the circumstances to ensure any overseas recipient of personal information does not breach the Australian Privacy Principles. The School accepts this requirement, and will seek the prior consent of the individual or their parent/guardian, as appropriate, should a disclosure of personal information to an overseas recipient be required.

As at February 2018, the School has Round Square student exchanges, conferences, and service trips that require the disclosure of student and staff personal information to overseas recipients, which are almost without exception other schools, or educational related entities in the following countries. This list will expand and appropriate scrutiny will apply, as new countries are included.

Cambodia	France	Indonesia	New Zealand	Thailand
Canada	Germany	Japan	Reunion Island	Turkey
China	Great Britain	Jordan	Scotland	United States of America
Columbia	India	Malaysia	South Africa	Vietnam

COMPLAINTS

How an individual may complain about a breach of the Australian Privacy Principles that bind the School, and how the School will deal with such a complaint.

Any complaint relating to the School's compliance with the Australian Privacy Principles must be addressed in writing directly to the Head of School. Such matters may include, but not be limited to, the School's refusal to provide access to an individual's personal information or refusal to correct an individual's personal information.

If the subject of complaint remains unresolved to the individual's satisfaction and the Head of School has been formally advised that the individual intends to take the issue to the School's Board of Governors, the individual can write to the Chair of the Board to complain formally. The only exception would be in the case of the Head of School being the subject of complaint, in that circumstance alone, an individual could bypass the Head of School and write directly to the Board Chair.

If the subject of complaint is still unresolved after discussion with the Board Chair, the individual must accept that their complaint has been heard and cannot be resolved, as they would wish it to be resolved by the School.

If the individual is not satisfied with the outcome offered by the School, the individual may make a complaint to the Australian Information Commissioner under section 36 of the Privacy Act.

Additional information on the Australian Privacy Principles and the Office of the Australian Information Commissioner is available at www.oaic.gov.au.

ANNEXURE DATA BREACH

NOTIFIABLE DATA BREACHES SCHEME (NDB Scheme)

The NDB Scheme was inserted into the Privacy Act 1988 by the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth). Effective 22 February 2018, it imposes an obligation on the School to notify affected individuals, whose personal information is involved in a data breach and that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner must also be notified of eligible data breaches (EDB) by the School by completing a Notifiable Data Breach Form.

DEFINITIONS

Eligible Data Breach

Concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information or the loss of personal information where the loss is likely to result in unauthorised access or disclosure.

A Data Breach is an Eligible Data Breach (EDB) if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach. The following three criteria need to be satisfied:

a. there is unauthorised access or unauthorised disclosure of personal information, or a loss of personal information that the School holds;
b. this is likely to result in serious harm to one or more individuals; and
c. the School has not been able to prevent the likely risk of serious harm with remedial action.

Not all Data Breaches will be EDBs, particularly where the School acts quickly to remediate a Data Breach, and because of this action, the data breach is not likely to result in serious harm. There is no obligation to notify the Information Commissioner or the individual(s).

Unauthorised access

Where personal information is accessed by someone, who is not permitted access, that is, by an employee of the School, an independent contractor, or a third party by 'hacking'.

Unauthorised disclosure

Where the School, intentionally or unintentionally, makes personal information accessible or visible to others outside the School and releases this information in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by a staff member.

Loss

Accidental or inadvertent loss of personal information held by the School, in circumstances where is it is likely to result in unauthorised access or disclosure.

Serious harm

Whether a data breach is likely to result in serious harm is an objective assessment. The **test** is whether a **reasonable man**, in the position of the School, would think that the data breach is likely to result in serious harm to the person whose personal information was part of the breach. Serious harm is not defined in the Privacy Act. It includes serious physical, psychological, emotional, financial, or reputational harm.

Examples

Data Breaches are not limited to the malicious acts of third parties, such as theft or 'hacking', but may also arise from human error, a system failure, or a failure to follow information handling or data security policies resulting in accidental loss, access, or disclosure.

The following are examples of when a Data Breach may occur:

a. loss of smartphone or other School device or equipment containing personal information;
b. cyber-attacks on the School's systems, resulting in unknown third parties accessing or stealing personal information;
c. accidental transmission of personal information such as student's reports to unintended recipients by e-mail;
d. loss or theft of hard copy documents; and
e. misuse of personal information of students or parents by School personnel.

ANNEXURE – FLOWCHART OF REPORTING OF ELIGIBLE DATA BREACH

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

Contain a suspected or known Data Breach where possible

ACCESS

The School 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 the School must notify the individuals affected and the Information Commissioner.

If the School only has grounds to suspect that this is the case then it must conduct an assessment. As part of the assessment, the School should consider whether remedial action is possible.

Initiate	Plan the assessment and assign a 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 evaluation.

The School must conduct the assessment expeditiously and preferably within 30 days. The School will document why it cannot be done within this period, if it is the case.

REMDEDIAL ACTION

Where possible, the School should take steps to reduce any potential harm to individuals.

Steps such as recovery of the lost information before it is accessed or changing access controls on accounts before unauthorised transaction can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and the School can progress to the review stage.

NO **IS SERIOUS HARM STILL LIKELY?** **YES**

Notify OAIC

Where serious harm is likely, the School must prepare a statement for the Commission that contains:

- The School's Name and Contact Details
- Description of the Data Breach
- Kind(s) of information concerned
- Recommended steps for individuals affected

Notify INDIVIDUALS

Inform the affected individuals of the contents of the OAIC statement; provide further information, where appropriate, such as an apology and an explanation of what steps are/have been taken.

Option 1	Notify ALL individuals
Option 2	Notify ONLY those individuals AT RISK of serious harm

If neither of these options is practicable then:

Option 3	The School will publish the statement on the School's website and publicise it.

REVIEW

The School will review the incident and take action appropriate in the circumstances to prevent future Data Breaches, which may include:

- Full investigation of the cause of the Data Breach
- Develop a prevention plan
- Conduct an audit
- Update security
- Change policies and processes
- Revise staff training practices

The School may also consider reporting the incident to other relevant bodies such as:

- Police or law enforcement
- External or third parties such as the ATO, SCSA
- Australian Cyber Security Centre and related bodies
- Credit Card companies or financial services providers

ANNEXURE – DATA BREACH RISK ASSESSMENT FACTORS

Who is the Personal Information about	
Who is affected by the breach	Students, Parents, Staff, Contractors, Service Providers, Other Agencies. The release of a student's personal information may be more serious than that of a contractor.
What kind of personal information is involved	
Does the type of personal information create a greater risk of harm	Certain information, such as sensitive information (health records) may pose a greater risk of harm to the affected individual(s) versus names and addresses that are in the public domain.
What is the context of the affected information and the breach	
What is the context of the personal information	Is it a list of students' names who attended a sporting event, or did they make use of a counselling service, asthmatic etc.
How long has the information been accessible	The length of time between the data breach occurring and the discovery, may be relevant to establishing what the likelihood is of serious harm resulting.
Who has accessed this information	Access or disclosure to a trusted and known party vs a party suspected of being involved in criminal activity.
Have there been other breaches that could have a cumulative effect	A number of minor, unrelated breaches may not create a real risk of serious harm, but when the cumulative effect of these breaches is considered, may meet this threshold. This could involve incremental breaches of the same School database, or known breaches from multiple different sources (e.g. multiple schools or multiple data points within the one school).
How could the personal information be used	Consider the purposes for which the information could be used, such as to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally. What is the risk of harm to the individual if the compromised information, along with other easily available information, is made public?
Establish the cause and the extent of the breach	
Is there a risk of ongoing exposure	What is the risk of repeated access, use or disclosure via mass media or online.
Evidence of an intention to steal personal information	Consider theft of a laptop to obtain the item vs intent to access the information thereon.
Is the personal information encrypted or not easily accessible	Are the measure to render the information unreadable? If so the risk is lessened.
Source of the breach	External vs internal Malicious (hacking) vs Unintentional (processing error) Lost information vs Stolen information Breach is intentional vs accidental
Has the information been recovered	Return of a laptop – any evidence of tampering
Steps to mitigate harm	School needs to assess and contain the breach – reset password, notification to affected individuals
Is this a systemic problem or an isolated incident	When identifying the source of the breach, need to assess whether there have been similar occurrences. This may suggest a systemic issue and therefore a greater risk.
Number of individuals affected	If the breach is systemic then more individuals may be affected. The scale of the breach may lead to a greater risk that the information will be misused and the response from the School needs to be proportionate. Nevertheless, a breach may be serious even if only a few individual s are affected.
Asses the risk of harm to the affected individual(s)	
Who is the information about	Some individuals are more vulnerable and less able to take steps to protect themselves, such as younger students, students with disabilities/special needs, vulnerable families, or parents.
What kind 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 students who attend the School may not be sensitive information. However, the same information about students 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: • encrypted electronic information; • information that the School could likely use to identify an individual, but that other people likely could not (such as a student number that only the School); and • information that has been adequately destroyed and cannot be retrieved to its original form e.g. 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 applies, the School may need to consider the likelihood of the encryption algorithm being broken in the long term.
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 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 criminal activity, or someone who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a student'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 students' domestic circumstances may be used to bully or marginalise the student 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 harm could result from the breach, including harm to the School?	Examples include loss of public trust in the School, 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 – DATA BREACH 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 be kept of the Data Breach and the response. Legal advice should also be sought if necessary.

Phase 1: Confirm, contain and keep records of the Data Breach and do a preliminary assessment

1. The member of School staff who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify the Head of Primary (Primary School), Head of Secondary (Secondary School), Boarding (Head of Boarding), or Bursar (Support Staff). 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. The Head of Primary, Head of Secondary, Head of Boarding, or Bursar, in consultation with the Head ICT, will make a preliminary assessment of the risk level of the Data Breach. The following table sets our examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information have been leaked externally. Example is health information.
Medium	Loss of some personal information records and the records do not contain sensitive information. A 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. Near miss or potential event occurred. No identified loss, misuse, or interference of personal information. Example is an email accidentally sent to the incorrect recipient.

4. Where a High Risk incident is identified, the Head of School will be notified in accordance with the School's Crisis Response Plan (POL-060), who will call a meeting of the staff relevant to the particular matter.

5. All High and Medium Risk Data Breaches must be escalated to the School's Crisis Response Group to consider if any of the affected individuals should be notified immediately where serious harm is likely.

6. If it is likely that there could be media or stakeholder attention because of the Data Breach, it must be escalated to the Head of School.

Phase 2: Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely

1. The Crisis Response Group will take any further steps available to contain the Data Breach and mitigate or remediate harm to affected individuals.

2. The Crisis Response Group will 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 Crisis Response Group will 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 Crisis Response Group should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB, such as Eligible data breaches of other entities, Enforcement related activities, Inconsistency with secrecy provisions, Declarations by the Commissioner.

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

1. The Crisis Response Group 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.

2. As soon as the Crisis Response Group 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.

3. After completing the statement, unless it is not practicable, the Crisis Response Group 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.

4. If it is not practicable to notify some or all of these individuals, the Crisis Response Group must publish the statement on their website, and take reasonable steps to publicise otherwise the contents of the statement to those individuals.

Phase 4: Take action to prevent future Data Breaches

The Crisis Response Group 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.

1. The Head of School will direct that the details of the Data Breach and response taken be entered into a Data Breach log. In addition, the Data Breach log will be reviewed annually, to identify any reoccurring Data Breaches.

2. The Head of ICT 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.

3. Where necessary, the Head of ICT, or the Crises Response Group, must recommend to the Head of School, any appropriate changes to policies, procedures and staff training practices, including updating the School's Data Breach Response Protocol.

4. If appropriate, the Head of ICT must 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.

FAQS

An email sent to an incorrect recipient

If the *recipient is a member of staff*, a request to them that they do not open the email or any attachments and then delete the email and do no discuss the information, is sufficient.

If the recipient were a *member of the wider community*, then *you would need to consider*:

- who was the email sent to (other students, parents)
- what type of personal information was in the email (is it a list of names of students attending an excursion, or is the information more sensitive such as health, disability, special needs, school results, pastoral concerns, financial)
- what is the likelihood of accessing this information causing serious harm, be this financial, emotional, reputational

Perhaps an email was sent to the parents of a year group providing details of an excursion and included a list of the students attending, then an email to the recipients explaining the error and requesting that they ignore the contents and delete the email confines the breach.

If the contents of the email included sensitive, health information, then the data breach should be escalated to the appropriate Head. This data breach may be damaging to both the student(s) identified and their parents. The School would immediately send an email to the parents, emailed in error, asking them not to open the attachment, to delete the email, and not to divulge the contents of the attachment if they had read it. The School would contact the parents of the student(s) identified, notifying them of what had occurred and what steps they had taken to remediate the harm, and what steps they were taking to prevent a reoccurrence in the future. As there was a risk of serious harm due to the wide distribution of the information, the sensitivity of the information, and the potential vulnerability of the family, the Information Commissioner would also be notified.

Loss of hard copy personal information

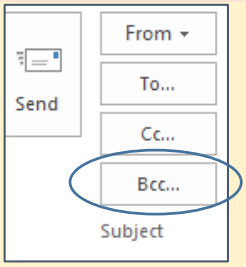
On returning from a trip, you realise the list of names of students in the class was left on a hired bus. Following a call to the bus company, it appears that they cannot find the list. The list had names and no other details. The kind of information indicates that serious harm was not likely to occur and no further action is necessary.

If the list contained health or other sensitive information, then the data breach should be escalated to the appropriate Head and, following an assessment of the nature of the information and the likelihood of serious harm resulting, the parents of the students and the Commissioner may need to be informed of the data breach.

Loss of a smartphone, laptop, iPad

There is the possibility that emails and personal information held by the School could be accessed on this device. Where the device is School property, contact the School's ICT staff and ask that they remotely delete the information and render the device unusable. Due to the security measures (passwords) on the device and the action by the ICT staff, the personal information is secure.

Good Practice

Laptop/ Desktop/ IPad	• Make it a practice to lock your device when you are away from your desk. • Laptops and IPads are provided for school use and should not be available for use by other members of staff (unless logged in on their account), or by family members. • Set up a screensaver. Inactivity will trigger the screen saver and hide personal information on the screen.
Filing Cabinets	• Files or notes with personal information should be in drawers or filing cabinets, particularly after hours.
Email	• Unlike SEQTA or Synergetic, which defaults to hide recipient email addresses, Outlook does not. Using the blind copy option when sending bulk emails is the best way to ensure privacy of email addresses.  • Do not open spam and report suspicious email to ICT Helpdesk (e.g. ATO refund emails).
Passwords	• Keep these current and ensure that the password is strong.

	• A strong password is between 12 and 14 characters, includes numbers, symbols, and a mixture of upper and lower case letters, and does not rely on obvious substitutions like a zero for O.
Secure Disposal	• When information is no longer required, take reasonable steps to destroy or de-identify the personal information. Ordinary disposal or recycling is not secure and is only suitable for documents already in the public domain. • There are secure disposal bins in various locations on campus, including Staff Centre. In addition, there are light-duty shredders in both Primary and Secondary Administration, along with a heavy-duty shredder in Finance.