ST. ANDREW'S GRAMMAR

PRIVACY POLICY

Date	*Modified By*	*Ratified*	*Review*
March 2006	Principal	2006	2007
November 2009	No change	N/A	2010
March 2010	No change	N/A	2011
March 2014	Principal	2014	2015
June 2017	Principal	2017	2018
May 2018	Principal	Board 2018	2019

Print Date: 7 May 2018

Introduction and Policy Statement

This Privacy Policy sets out how St Andrew's Grammar manages personal information provided to or collected by the School.

This Policy also details how we protect your privacy and how we comply with the requirements of the Privacy Act and the 13 Australian Privacy Principles. It also describes:

- From whom we collect information;
- the types of personal information collected and held by us;
- how this information is collected and held;
- the purposes for which your personal information is collected, held, used and disclosed;
- how you can gain access to your personal information and seek its correction;
- how you may complain or inquire about our collection, handling, use or disclosure of your personal information and how that complaint or inquiry will be handled; and
- whether we are likely to disclose your personal information to any overseas recipients.

The School will review and update this Privacy Policy annually to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

From whom do we collect Personal Information?

At St. Andrew's Grammar we collect personal information from:

- students;
- parents;
- prospective parents;
- job applicants;
- staff;
- volunteers; and
- others including alumni, contractors, visitors and others that come into contact with the school.

It is noted that employee records are not covered by the Australian Privacy Principles where they relate to current or former employment relations between the school and the employee.

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

The type of information the School collects and holds includes (but is not limited to):

- Personal Information including names, addresses and other contact details; dates of birth; next of kin details; financial information, photographic images and attendance records.

- Sensitive Information (particularly in relation to student and parent records) including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional or union memberships, family court orders and criminal records.

- Health Information (particularly in relation to student and parent records) including medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

Detailed examples of what is collected includes:

1) Students and parents and/or guardians before, during and after the course of a student's enrolment at the School, including:
   - name, contact details (including next of kin), date of birth, previous school and religion;
   - medical information (e.g. details of disability and/or allergies, Absence notes, medical reports and names of doctors);
   - conduct and complaint records, or other behaviour notes, and school reports;
   - information about referrals to government welfare agencies;
   - counselling reports;
   - health fund details and Medicare number;
   - any court orders;
   - volunteering information; and
   - photos and videos at School events;

2) Job applicants, staff members, volunteers and contractors, including:
   - name, contact details (including next of kin), date of birth, and religion;
   - information on job application;
   - professional development history;
   - salary and payment information, including superannuation details;
   - medical information (e.g. details of disability and/or allergies, and medical certificates)
   - complaint records and investigation reports;
   - leave details;
   - photos and videos at School events;
   - work emails and private emails (when using work email address) and Internet browsing history

3) 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.

More accurately, how we collect personal information will largely be dependent upon whose information we are collecting. If it is reasonable and practical to do so, we collect personal information directly from you.

Where possible the school has attempted to standardise the collection of personal information by using specifically designed forms (e.g. the Enrolment Form). However, given the nature of our operations, we often also receive personal information by email, letters, notes, over the telephone, in face to face meetings, through financial transactions and through our surveillance activities such as the use of CCTV security cameras or email monitoring.

We may also collect personal information from other people (e.g. a personal reference) or independent sources (e.g. a telephone directory), however we will only do so where it is not reasonable and practical to collect the information from you directly.

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 or a reference from another school.

Sometimes we may be provided with your personal information without having sought it through our normal means of collection. We refer to this as "unsolicited information". Where we collect unsolicited information we will only hold, use and/or disclose that information if we could otherwise do so had we collected it by normal means.

If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the information as appropriate.

How will the School use the personal information you provide?

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

Students and Parents:

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

The purposes for which the School 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 the School;

- looking after students' educational, social and medical wellbeing;

- seeking donations and marketing for the School; and
- to satisfy the School's legal 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 provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

Job applicants and contractors:

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

The purposes for which the School uses personal information of job applicants and contractors include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking donations and marketing for the School; and
- satisfying 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 conduct associated activities, 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 organisations that assist in the School's fundraising, for example, the School's 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.

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

The School may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools;
- government departments;

- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, coaches, volunteers, counsellors and providers of learning and assessment tools;
- assessment and educational authorities, including the WA School Curriculum and Standards Authority (SCSA) and the Association of Independent Schools of WA (AISWA);
- people providing administrative and financial services to the School;
- recipients of School publications, such as newsletters and magazines;
- students, parents or guardians;
- anyone you authorise the School to disclose information to; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Sending and storing information overseas:

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

- obtaining the consent of the individual; or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The School may use online or 'cloud' service providers to store personal information and to provide services to the School that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

An example of such a cloud service provider is Microsoft. Microsoft provides Office365 including email and document storage and also stores and processes limited personal information for this purpose. School personnel and the Hellenic Administration and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering Office 365 and ensuring its proper use.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

Storage, management and security of personal information

The School's staff are required to respect the confidentiality of students and parent's personal information and the privacy of individuals. No student names are to be shown in the subject line of any email.

The School has in place steps to protect the personal information the School holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

We store personal information in a variety of formats including on databases, in hard copy files and on personal devices including laptop computers, mobile phones, cameras and other recording devices.

The security of your personal information is of importance to us and we take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure.
These steps include:

- Restricting access to information on the school databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where sensitive and health information is stored in hard copy files that these files are stored in lockable cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures around the school buildings and grounds to prevent break-ins.
- Implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, confidentiality and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Personal information we hold that is no longer needed is destroyed in a secure manner, deleted or de-identified as appropriate.

Our website and online publications such as the School Newsletter, may contain links to other websites. We do not share your personal information with those websites and we are not responsible for their privacy practices. Please check their privacy policies.

Access and correction of personal information

Under the Commonwealth Privacy Act an individual has the right to seek and obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. Students will generally be able to access and update their personal information through their parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or to update any personal information the School holds about you or your child, please contact the School Principal by telephone (9376 5850) or in writing. The School may require you to verify your identity and specify what information you require.

The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

Consent and rights of access to the personal information of students

The School respects every parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The School 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.

Parents may seek access to personal information held by the School about them or their child by contacting the Principal by telephone or in writing. However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

We are however cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students.

We also acknowledge that there may be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others or result in a breach of the school's duty of care to the student.

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 warrant it.

How we ensure the quality of your personal information

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date. These steps include ensuring that the personal information is accurate, complete and up to date at the time of collection and when using or disclosing the personal information. On an ongoing basis we maintain and update personal information when we are advised by individuals or when we become aware through other means that their personal information has changed.

Please contact us if any of the details you have provided change. You should also contact us if you believe that the information we have about you is not accurate, complete or up to date.

Enquiries and complaints

If you would like further information about the way St. Andrew's Grammar manages the personal information it holds, or wish to complain that you believe that the School has breached the Australian Privacy Principles please contact the Principal in writing (enrolments@sag.wa.edu.au) or by telephone (9376 5850).

The School will investigate any complaint and will notify you of the decision in relation to your complaint as soon as is practicable after it has been made.

Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website (www.sag.wa.edu.au) regularly for any changes.

DISCLOSURE STATEMENT TO STUDENTS

Counselling at St Andrew's Grammar – Things You Should Know

The School provides counselling services for its students as part of its pastoral care program.

These are provided through the AISWA Non-Government School Psychology Service.

A referral to the AISWA Non-Government School Psychology Service can only be made by the Principal, Head of Primary, Academic Director or Coordinator of Pastoral Care Years 7-9.

There are a number of things that students and their parents should know before using the counselling service.

1) The School is very conscious of the need for confidentiality between Counsellor and student. However, at times it may be necessary for the Counsellor to divulge the contents of discussions or records to the Principal, if the Principal or the Counsellor considers it necessary for the student's welfare to discharge the School's duty of care to the student.

2) It is also possible that the Principal may need to disclose aspects of discussions with Counsellors to others in order to assist the student.

3) Where a disclosure is made it would be limited to those who need to know, unless the student consents to some wider disclosure.

We emphasise that disclosures (if any) would be very limited. However, if a student is not prepared to use the counselling services on the basis set out above, the student will need to obtain counselling services from outside the school.

ST ANDREW'S GRAMMAR

PHOTOGRAPH/VIDEO PERMISSION FORM

Dear Parent/Guardian,

At certain times throughout the year, our students may have the opportunity to be photographed or filmed for our school publications, such as the school's newsletter or website and social media, or to promote the school in newspapers and other media.

We would like your permission to use your child's photograph/video for the above purposes. Please complete the permission form below and return to the school as soon as possible.

Thank you for your continued support.

STUDENT'S NAME: _____ YEAR LEVEL: _____

I give permission for my child's *photograph/video* be published in:

- ☐ the school website
- ☐ social media
- ☐ promotional materials
- ☐ newspapers and other media

I give permission for my child's name to be published in:

- ☐ the school website
- ☐ social media
- ☐ promotional materials
- ☐ newspapers and other media.

I understand and agree that if I do not wish to consent to my child's photograph/video appearing in any or all of the publications above, or if I wish to withdraw this authorisation and consent, it is my responsibility to notify the school.

Licensed under NEALS: The photograph/video may appear in material which will be available to schools and education departments around Australia under the National Educational Access Licence for Schools (NEALS), which is a licence between education departments of the various states and territories, allowing schools to use licensed material wholly and freely for educational purposes.

Name of Parent / Guardian _____

Signed: Parent/Guardian _____Date: _____

If Student is aged 15+, student must also sign:

Signed: Student_____ Date: _____

Any personal information will be stored, used and disclosed in accordance with the requirements of the Privacy Act 1988 (Cth).

OFFICE USE
Date of Photograph/Video: (month & year)

PRIVACY BREACH RISK ASSESSMENT FACTORS

Consider the type of personal information involved	
Does the type of personal information create a greater risk of harm?	Some information, such as sensitive information (e.g. health records) or permanent information (e.g. date of birth) may pose a greater risk of harm to the affected individual(s) if compromised. A combination of personal information may also pose a greater risk of harm.
Who is affected by the breach?	Are students, parents, staff, contractors, service providers, and/or other agencies or organisations affected? For example, a disclosure of a student's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.
Determine the context of the affected information and the breach	
What is the context of the personal information involved?	For example, a disclosure of a list of the names of some students who attend the School may not give rise to significant risk. However, the same information about students who have attended the counselling support or students with disabilities may be more likely to cause harm. The disclosure of names and address of students or parents would also create more significant risks.
Who has gained unauthorised access to the affected information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher at another school gains unauthorised access to a student's name, address and grades without malicious intent (e.g. if the information is accidentally emailed to the teacher), the risk of serious harm to the student may be unlikely.
Have there been other breaches that could have a cumulative effect?	A number of minor, unrelated breaches that might not, by themselves, create a real risk of serious harm, may meet this threshold when the cumulative effect of the breaches are considered. 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. For example, could it be used to commit identity theft, commit financial fraud, abuse the individual either physically or emotionally (including to humiliate the affected individual and social or workplace bullying)? For example, information on students' domestic circumstances may be used to bully or marginalise the student and/or parents. What is the risk of harm to the individual if the compromised information can be easily combined with other compromised or publicly available information?
Establish the cause and extent of the breach	
Is there a risk of ongoing breaches or further exposure of the information?	What is the risk of further repeat access, use or disclosure, including via mass media or online?
Is there evidence of intention to steal the personal information?	For example, where a mobile phone has been stolen, can it be determined whether the thief specifically wanted the information on the phone, or the phone itself? Evidence of intentional theft of the personal information (rather than just the device on which it is stored) can suggest an intention to cause harm, which may strengthen the need to notify the affected individual, as well as law enforcement.
Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?	Consider whether the information is rendered unreadable by security measures or whether the information is displayed or stored in way that renders it unusable if breached. If so, the risk of harm to the individual may be lessened.
What was the source	For example, was it external or internal? Was it malicious or unintentional? Did it

of the breach?	involve malicious behaviour or was it an internal processing error (such as accidentally emailing a student list to an unintended recipient)? Was the information lost or stolen? Where the breach is unintentional or accidental, there is likely to be less risk to the individual than where the breach was intentional or malicious.
Has the personal information been recovered?	For example, has a lost mobile phone been found or returned? If the information has been recovered, is there any evidence that it has been accessed, copied or tampered with?
What steps have already been taken to mitigate the harm?	Has the School fully assessed and contained the breach by, for example, replacing comprised security measures such as passwords? Are further steps required? This may include notification to affected individuals.
Is this a systemic problem or an isolated incident?	When identifying the source of the breach, it is important to note whether similar breaches have occurred in the past. If so, there may be a systemic problem with system security, or there may be more information affected than first thought, potentially heightening the risk.
How many individuals are affected by the breach?	If the breach is a result of a systemic problem, there may be more individuals affected than initially anticipated. The scale of the breach may lead to a greater risk that the information will be misused, so the response must be proportionate. Although it is vital to remember that a breach can be serious despite affecting only a small number of individuals, depending on the information involved.
Assess the risk of harm to the affected individuals.	
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: (i) encrypted electronic information; (ii) information that the School could likely use to identify an individual, but that other people likely could not (such as a student number that only the School uses – this should be contrasted to a student number that is used on public documents); and (iii) information that has been adequately destroyed and cannot be retrieved to its original form (such as shredded hard copy information).
If the information is not in a form that is intelligible to an ordinary person, what is the likelihood that the information could be converted into such a form?	For example, encrypted information may be compromised if the encryption algorithm is out-of-date or otherwise not fit for purpose and could be broken by a sophisticated attacker, or if the decryption key was also accessed or disclosed in the breach. Even where none of these concerns apply, the School may need to consider the likelihood of the encryption algorithm being broken in the long term.
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	For example, could an attacker have overcome network security measures protecting personal information stored on the network?

likelihood that any of those security measures could be overcome?	
What persons (or kind of persons) have obtained or could obtain the information?	Access by or disclosure to a trusted, known party is less likely to cause serious harm than access by or disclosure to an unknown party, a party suspected of being involved in criminal activity or a party 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 to the student 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 pupil and/or parents.
In terms of steps to mitigate the harm, what is the nature of those steps, how quickly are they being taken and to what extent are they likely to mitigate the harm?	Examples of steps that may mitigate the 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 mitigating 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 Privacy Breach.
Assess the risk of other harms	
What other possible harms could result from the breach, including harms 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.

PRIVACY BREACH RESPONSE PROTOCOL

Introduction

This protocol sets out the procedure to manage the School's response to the actual or suspected misuse, interference, loss, or unauthorised access, modification or disclosure of personal information (Privacy Breach). It is intended to enable the School to contain, assess and respond to a Privacy Breach. The School will also seek guidance from AISWA and Lavan Legal.

Response protocol

In the event of a Privacy Breach, all School personnel must adhere to the following four phase process.

Phases 1 – 3 should occur in quick succession and may occur simultaneously.

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

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

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

Risk Level	**Description**
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information.
Low	Low Risk Privacy Breach, but there is an indication of a systemic problem in processes or procedures. A few names and school email addresses accidentally disclosed to a trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information

6. The Principal must make a preliminary assessment of the risk level of the Privacy Breach. This will involve an analysis of the risks involved. The above table sets out examples of the different risk levels.

7. In the event that the Principal receives multiple reports of Privacy Breaches of different datasets, this may be part of a related incident. The Principal must consider upgrading the risk level if this situation arises.

8. Where a High Risk incident is identified, the Principal must consider if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals.

9. The Principal must escalate High Risk and Medium Risk Privacy Breaches to the response team (whose details are set out at the end of this protocol).

10. If the Principal believes a Low Risk Privacy Breach has occurred, he will determine that the response team does not need to be convened. In this case, he must undertake Phases 2 and 3 below.

11. If there could be media or stakeholder attention as a result of the Privacy Breach, it must be escalated to the response team.

12. If appropriate, the response team should pre-empt media interest by developing a communications or media response and strategy that manages public expectations.

Phase 2. Evaluate the risks associated with the Privacy Breach

1. The response team is to take any further steps (i.e. those not identified in Phase 1) available to contain the Privacy Breach and mitigate harm to affected individuals.

2. The response team is to work to evaluate the risks associated with the Privacy Breach by:
    a. identifying the type of personal information involved in the Privacy Breach;
    b. identifying the date, time, duration, and location of the Privacy Breach;
    c. establishing the extent of the Privacy Breach (number of individuals affected);
    d. establishing who the affected, or possibly affected, individuals are;
    e. identifying what is the risk of harm to the individual/s and the extent of the likely harm (eg what was the nature of the personal information involved);
    f. establishing what the likely reoccurrence of the Privacy Breach is;
    g. considering whether the Privacy Breach indicates a systemic problem with practices or procedures;
    h. assessing the risk of harm to the School; and
    i. establishing the likely cause of the Privacy Breach.

3. The response team should assess priorities and risks based on what is known.

4. The response team does not need to consider a particular matter above if this will cause significant delay in proceeding to Phase 3.

5. The response team should regularly update each other and other relevant stakeholders regarding incident status.

Phase 3. Consider Privacy Breach notifications

1. Where appropriate, having regard to the seriousness of the Privacy Breach (based on the evaluation above), the response team must determine whether to notify the following stakeholders of the Privacy Breach:
    a. affected individuals;

b. parents;
c. the OAIC; and/or
d. other stakeholders (e.g. if information which has been modified without authorisation is disclosed to another entity, that entity may need to be notified).

2. In general, if a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals (and their parents if the affected individuals are pupils) then OAIC must be notified.

3. The response team will facilitate the completion and submission of a **Breach Response Form** to the OAIC.

Phase 4. Take action to prevent future Privacy Breaches

1. The response team must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3. The cause of the Privacy Breach must be fully investigated.

2. The response team must enter details of the Privacy Breach and response taken into a Privacy Breach log. The response team must every year review the Privacy Breach log to identify any reoccurring Privacy Breaches.

3. The response team must facilitate the completion and submission of a **Breach Response Form** to the OAIC.

4. The response team must conduct a post-breach review to assess the effectiveness of the School's response to the Privacy Breach and the effectiveness of the Privacy Breach Response Protocol.

5. The response team, if necessary, will make appropriate changes to policies, procedures and staff training practices, including updating this Privacy Breach Response Protocol.

6. The response team, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Privacy Breach and conduct an audit to ensure the plan is implemented.

Response Team

ROLE	**AREA**
Principal	School Management
Information Technology	I.T. Manager
Finance Administration	Co-ordinator of Finance Administration

Contacts

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

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

PRIVACY BREACH RESPONSE FORM

INTRODUCTION

The Privacy Amendment Act 2017 has introduced a mandatory data breach notification requirement for entities subject to the Privacy Act. An '*eligible data breach'* is arises when the following conditions are satisfied:

- If there is an unauthorized access to personal information.
- A situation where there is unauthorized disclosure or when is there is loss of personal information.

Either of these situations are likely to result in serious damage to the School or an individual. The new legislation demands that agencies, organisations and other certain entities to provide notice to the Australian Information Commissioner and affected individuals of certain data breaches. It's a statutory requirement for the School to report incidents of data breach.

TYPES OF DATA BREACH

- Information Security Breach – A breach that results in unauthorized access of data, services, applications and networks by bypassing through the security mechanism.
- Personal Health Information Breach – This breach occurs when personal health information is viewed, shared, stolen or removed by an unauthorized individual.
- Corporate, Financial or Medical Workforce Information Breach – When there is unauthorized access to human resources system, bank details of staff and pay slips details. It also includes publishing of budget related information leak of professional development documentation.

DATA BREACH RESPONSE

Data breaches must be dealt by a proper assessment of the risks involved and using the risk to plan the future course of action. Security methods must be aligned with the importance and the sensitivity of the information.

Initiating A Preliminary Assessment

- Follow the **Privacy Breach Response Protocol.**

Evaluate The Impact of the Breach and Risk to Individuals

- Evaluate the impact and the risk to the School and individual related with the breach. The following factors should be kept in mind:
  - The context of the affected information and breach.
  - The type of personal information involved e.g. health information, contact information and financial information.
  - The major causes of the breach and the extent of the breach.

Breach Notification

- Depending upon the extent of the breach, notification should be provided to the following authorities:
  - The Australian Information Commissioner
  - The Police
  - The School Board

- The Department of Education- Critical Incident Report
- The Corruption and Crime Commission
- Other agencies and individuals directly affected by the breach.

Review and Response

- The School will ensure that the cause of the breach has been fully investigated and recommendations and outcomes will be determined. Necessary training of staff will be undertaken if possible and amendments will be made to all relevant policies and the procedures.

ST. ANDREW'S GRAMMAR DATA BREACH INCIDENT FORM

This section is to be completed to inform the AUSTRALIAN INFORMATION COMMISSIONER and other entities about an 'eligible data breach'. Notifying the Authorities:

TICK YES OR NO

AUSTRALIAN INFORMATION COMMISSIONER

Y	N

POLICE

Y	N

THE SCHOOL BOARD

Y	N

THE DEPARTMENT OF EDUCATION – CRITICAL INCIDENT REPORT

Y	N

THE CORRUPTION AND CRIME COMMISSION

Y	N

INFORMATION INVOLVED IN THE DATA BREACH:

Please select the ones which apply: WRITE YES (if applicable)

- Health Information _____
- Contact Information (e.g. Home Address, Phone Number, Email address_____
- Financial Information _____
- Government identification (e.g. Centrelink Number, Medicare Number _____
- Superannuation Details or Tax File Number _____
- Other Information (Please Specify) _____

REPORTED BY: _____ DATE OF REPORT: _____

TITLE / ROLE: _____ INCIDENT NO.: _____

INFORMATION SECURITY INCIDENT INFORMATION

DATE OF INCIDENT: _____ TIME OF INCIDENT: _____

INCIDENT MANAGER: _____ TITLE / ROLE: _____

PHONE: _____ EMAIL: _____

LOCATION: _____

SPECIFIC AREA OF LOCATION *(if applicable):* _____

INCIDENT TYPE: _____

NO. OF HOSTS AFFECTED: _____ SOURCE IP ADDRESS: _____

IP ADDRESS: _____ COMPUTER / HOST: _____

OPERATING SYSTEM: _____ OTHER APPLICATIONS: _____

HOW DID THE BREACH OCCUR

IMPACT ASSESSMENT:

RESULTING DAMAGE:

IMMEDIATE ACTION TAKEN:

PLANNED ACTION AND RESULTING PREVENTATIVE MEASURES:

ADDITIONAL INFORMATION:

DATA BREACH IMPACT RATING

1. NEGLIGIBLE 2. LOW 3.MEDIUM 4.HIGH

SELECT THE IMPACT LEVEL

Please provide reason for the allocation:

ASSESSMENT OF THE LEVEL OF RISK

	NEGLIGIBLE	LOW	MEDIUM	HIGH	COMMENTS
RISK TO SAFETY	No or minimal risk to organisation / individual	Low risk to organisation / individual safety	Multiple or moderate risk to organsisation/ individual safety	High risk to organisation / individual safety	
LOSS OR DAMAGE TO	Negligible or very low damage and disruption to business	Minor damage / visible to the public and moderate disruption	Big loss to entity and individual both / measureable damage	Long term loss and adverse effect on reputation	
RESPONSE	Routine internal reporting required	Investigation required and notifications to individuals	Immediate investigation/ review of policy and investigations	Shut down of service/ immediate action required	
OFFENCE PUNISHMENT & FINE	Breach offence punishable by a small fine	Offence punishable by a moderate fine	Major fine and subsequent penalties	Offence punishable by imprisonment	

INFORMATION SECURITY INCIDENT INFORMATION SHARING		
INDIVIDUALS REQUIRING NOTIFICATIONS	POINT OF CONTACT NAME	DATE OF NOTIFICATION

REPORTING STAFF NAME: _____ REPORTING STAFF SIGNATURE: _____ DATE: _____

SUPERVISOR NAME: _____ SUPERVISOR SIGNATURE: _____ DATE: _____

If the data breach mentioned above was also a data breach of any other organization, you may need to provide their details.

Please tick Yes or No

Y	N

Please provide the contact information of the other affected entity:

ENTITY NAME	
CONTACT NUMBER	
ADDRESS	
SUBURB	
STATE	
OTHER CONTACT DETAILS	