Privacy Policy & Procedure

Updated November 2019

POLICY OWNER: Headmaster

PRIVACY POLICY & PROCEDURE

PURPOSE:	The following document outlines the policy of St Peter's College on the use and management of personal information provided to or collected by the School. The School acts in accordance with the Australian Privacy Principles contained in Schedule 1 of the Privacy Act 1988 (Cth) ("Act"). The School may, from time to time, review and update this Privacy Policy to take account of new laws (including amendments to the Act) and technology, changes to the School's operations and practices, and to make sure it remains appropriate to the changing school environment.
SCOPE:	This policy also defines St Peter's College procedures for implementing Mandatory Reporting where personal information is managed inappropriately and/or an eligible data breaches occurs as required in The Privacy Amendment (Notifiable Data Breaches) Act 2017.
RESPONSIBILITY AND CONTACT DETAILS:	All staff (past and present), students, parents and old scholars of St Peter's College and members of the community in general are covered by this policy. As required by the Act, the School has appointed a Privacy Officer who will oversee the implementation of this policy and be the point of contact for queries relating to the collection and handling of personal information. The role of the Privacy Officer will be undertaken by the Director of Finance and Administration who can be contacted by phone via Reception.
REFERENCES:	**Privacy Act 1988 (Cth)** **Summary of Australian Privacy Principles contained in Schedule 1 of the Act:** **APP 1 – Open and transparent management of personal information** Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy. **APP 2 – Anonymity and pseudonumity** Requires APP entities to give individuals the option of identifying themselves, or of using a pseudonym. **APP 3 – Collection of solicited personal information** Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information. **APP 4 – Dealing with unsolicited personal information** Outlines how APP entities must deal with unsolicited personal information. **APP 5 – Notification of the collection of personal information** Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters. **APP 6 – Use or disclosure of personal information** Outlines the circumstances in which an APP entity may use or disclose personal information that it holds. **APP 7 – Direct marketing** An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. **APP 8 – Cross-border disclosure of personal information** Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information
Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information
Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

DEFINITIONS

SPC: St Peter's College

Personal information: is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not that information or opinion is true and regardless of how it is recorded. St Peter's College collects personal information about our students, families, teachers, suppliers, job applicants, staff members (past and present), volunteers and contractors. It can also include other people who come into contact with the School, e.g. donors to the School or its associated bodies, including the Old Scholar's Association, and The St Peter's College Foundation Inc. ('Foundation').

Personal information includes information about students and parents and/or guardians ('parents') for example, names, addresses, telephone numbers, email addresses, dates of birth, passport numbers and photographs. It can be collected and held before, during and after the course of a student's enrolment at the School, including when students become old scholars.

Sensitive Information: a subset of personal information, includes the following, amongst other matters:

- information or an opinion about an individual's racial or ethnic origin, religious beliefs or affiliations, political opinions, sexual orientation or practices or criminal record;
- health information;
- genetic information that is not otherwise health information; and
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

Data breach: when personal information held by St Peter's College is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

Data breaches can occur in a number of ways. Some examples include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- hard disk drives and other digital storage media being disposed of without erasing contents
- databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the St Peter's College
- employees, volunteers or contractors accessing or disclosing personal information outside the requirements or authorisation of their employment or association to the School
- paper records stolen from insecure recycling or garbage bins
- St Peter's College mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and
- an individual deceiving St Peter's College into improperly releasing the personal information of another person.

Possible data breaches may be identified in a number of ways, internally (by staff, students, contractors, etc.) or externally (by community members, suppliers, via the School's Complaints Process, by other third parties, etc.)

ALIGNMENT TO SCHOOL STRATEGIC PLAN:

Towards a Preferred Future – A Strategic Plan for St Peter's College 2011 – 2014 underpins this policy & procedure.

POLICY:

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

The School will generally collect personal information (refer to definitions section) held about an individual by way of forms filled out by parents, students, job applicants, staff members, contractors and volunteers, face-to-face meetings and interviews, queries submitted to the School through its website or by email and telephone calls. The School or its contractors will collect personal information in the form of photographs and footage of students, parents and staff. The School will collect biometric information and biometric templates from photographs of students. On occasions people other than parents and students provide personal information about a student.

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

Personal information may be held in paper and electronic files. We take all reasonable steps to ensure that the information we collect is stored securely. The School is required by law to retain records for certain periods of time depending on the type of record and will comply with its legal obligations. These records may contain personal information of individuals.

The Australian Privacy Principles require the School not to store personal information longer than necessary. Accordingly, the School will dispose of records in accordance with acceptance standards and legislative requirements. Personal information is disposed of in accordance with accepted destruction standards, legal requirements as applicable and normal administrative practice, via a secure service provider.

If a person does not wish the School to collect certain information about them, they will need to advise the School's Privacy Officer. Any consequences this may have will be discussed with the individual.

Where St Peter's College receives, accesses or retains unsolicited personal information (i.e. personal information provided to St Peter's College which St Peter's College did not request) the information will be destroyed. No copies of the information will be retained.

Exception in relation to employee records

Under the Act the Australian Privacy Principles do not apply to an employee record (defined to mean a record of personal information relating to the employment of the employee). As a result, the practices described in this Privacy Policy do not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and employee. It is possible for an employee to engage with the School in multiple capacities (e.g. as an employee as well as a parent of a student). The employee records exception will be applied by the School accordingly, and when it is not relevant, the requirements of this Privacy Principle will apply.

How will the School use the personal information collected?

The School will use personal information it collects for the primary purpose of that collection, and for such other secondary purposes that are normally or might reasonably be related to the primary purpose of collection, or to which the individual has consented. In general, the School will collect, hold, use and disclose personal information for the purposes of providing educational services, to provide pastoral support, to maintain safety and wellbeing of students and related ancillary activities, including fundraising.

By providing the School with personal information, individuals consent to the School using and disclosing that personal information for the following purposes:

- providing that person with news and information about our products and services;
- sending you marketing and promotional material that we believe you may be interested in, either from us, any of our related entities (including the Old Scholar's Association and Foundation) or a third-party business which we consider may be of interest to you;
- personalising your experience with our activities, for example, via connectivity with social media services; and
- for job applicants and people tendering to provide goods or services to the School, assessing eligibility for employment by the School, or engagement by the School as a contractor.

Individuals may opt out of receiving marketing and promotional material from the School at any time by contacting the Privacy Officer.

Personal information collected from students and their parents will be used in the administration of a student's enrolment, academic progression through the School, graduation, the provision of services to students, parents and other school community members, and for related purposes in ways that you would reasonably expect to occur at a school like St Peter's College. This includes disclosure of information to the Old Scholar's Association, the Foundation. By providing personal information to us, individuals consent to this.

The Old Scholar's Association uses the personal information of former students to inform them about Old Scholar activities and for fundraising. Old scholars may update or amend their personal details by contacting the Alumni Officer.

The Foundation uses the personal information of parents and old scholars to provide them with marketing material and inform these parties of its fundraising activities, and seek their participation.

The School uses the personal information of students (including photographs, footage and names) for general marketing and promotional activities subject to receiving specific consent from the student or the student's parents.

Collection of Personal information

A **written** collection statement (as scripted in Appendix A) should be included on any document which requests personal information to be disclosed, in order to make the individual aware of the use of the personal information and security measures in place.

A **verbal** collection statement (as scripted in Appendix B) should be recited at the time of collection of personal information (or as soon as practicable afterwards) to make the individual aware of the use of the personal information and security measures in place.

Who might the School disclose personal information to?

St Peter's College staff are permitted to use and disclose personal information about an individual:

- for the primary purpose of the original collection of that personal information;
- if the individual consents to the use or disclosure of the personal information;
- for secondary purposes that the individual would reasonably expect the School to use or disclose the personal information for, where such secondary purpose is related (or, in the case of sensitive information, directly related) to the primary purpose of the original collection of the personal information; or
- for other specific purposes permitted under the Act, including as required by law.

The School will from time to time disclose personal information it holds to the Old Scholar's Association, the Foundation, the Collegians' Association and/or the Friends of Saints to enable them to undertake their activities and keep in touch with the School community.

In addition to the Old Scholar's Association, the Foundation, the Collegians' Association and the Friends of Saints, the School may be required to disclose some personal information to Courts, or Tribunals, or to State or Commonwealth government agencies to comply with other laws, for example, provide statistics, and for mandatory reporting to government departments. Personal information may also be required to be disclosed as part of evidence in Court or Court proceedings, including if the School is subpoenaed.

The School may disclose personal information it holds to its contractors to the extent necessary for the contractors to provide services to the School, subject to such contractors being contractually obliged to comply with the Act in respect of the personal information. This may include disclosure of sensitive information where a contractor is required to provide technical assistance to the School to enable the School to carry out the primary purpose of the original collection of the sensitive information.

The School may disclose personal information it holds in exceptional circumstances if it is considered imperative for reasons of health and safety.

The School may use personal information to contact parents regarding satisfaction surveys we conduct from time to time that help us to evaluate and improve our education services.

The School will seek consent from individuals prior to the use or disclosure of their personal information for purposes other than those described in this document.

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 schooling and educational services for the student. This includes satisfying both the needs of parents 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 include:

- pre-enrolment matters;
- to keep parents informed about matters related to their child's schooling, through correspondence, newsletters, magazines, other publications and the website;
- day-to-day administration;
- looking after students' educational, social and medical well-being;
- organising functions and other School activities;
- seeking donations for the School;
- promotion and marketing of the School; and
- to satisfy the School's legal obligations and allow the School to satisfy its duty of care.

In some cases where the School requests personal information about a student or parent and this is not supplied, the School may not be able to enrol or continue the enrolment of the student.

Job applicants, staff members 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, staff members and contractors include:

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

When a person applies for a position, or on commencement of employment at the School, they are asked to supply information to the School to enable processing of the person's employment and to maintain ongoing employment related functions. Generally this information includes: Name, Address, Telephone Number/s, Fax Numbers, Email address/s, Date of Birth, Gender, Citizenship, Ethnic origin, Passport Details, Disabilities, Health details, Web Address, Previous Employment details, Qualifications, Salary details, Bank Account details and Tax File numbers.

At the time information is being collected, staff will be advised if there is a legal requirement to supply the information requested (for example, if it is required by immigration or tax law).

Human Resources collects personal information as part the School's contractual relationships with individuals to ensure payment for employment services rendered.

Personal information collected or held by Human Resources will be used for managing processes associated with the employment relationship with the School. Activities may include payroll, human resource management,

superannuation, risk management (workers compensation insurance), recruitment and internal/external audits.

Personal information may also be used in statistical or aggregated forms for School planning, or for purposes required by Australian government bodies, for example, the Australian Taxation Office.

In general, the School will only disclose personal information to third parties if the staff member has authorised the third party (such as financial institutions or superannuation funds), to have access to personal information with the following exceptions:

- The School will disclose personal information when required to do so by law. This could be as a requirement to satisfy warrants, subpoenas, Court orders or Workers Compensation orders.
- The School may also disclose personal information to a third party if there are reasonable grounds to consider that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the staff member or another person.

The School will not sell, rent or trade staff members' personal information. Personal information is not released outside the School except in the circumstances described above.

No personal information about staff will be released to the media by Human Resources without the consent of the individual concerned and in consultation with the Communications & Marketing Department and in line with the School's Media Policy.

Volunteers

The School also obtains personal information about volunteers who assist the School in its functions or to conduct associated activities – such as the Friends of Saints - 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 be 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 St Peter's College Foundation, the Collegians' Association or the Friends of Saints.

Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information from the School or one of its associated organisations, including the Foundation. School publications, like newsletters, magazines and the website, which may contain personal information, may be used for marketing purposes.

How does the School treat sensitive information?

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 of disclosure or the sensitive information is allowed by law.

Management and security of personal information

The School's staff are required to respect the confidentiality of students' and parents' personal information and the privacy of individuals. All staff members are bound by a Confidentiality Agreement as part of their employment obligations.

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

Updating personal information

The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by contacting the School's main Reception or the Privacy Officer at any time.

Individuals have the right to check what personal information the School holds.

Under the Act, 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 and require its correction. There are some exceptions to this right set out in the Act.

Students will generally have access to their personal information through their parents, but older students may seek access themselves.

To make a request to access any information the School holds about an individual (or that person's child, if a parent), that individual should contact the Privacy Officer in writing.

The School may require the individual to verify their identity and specify what information is required. The School may charge a fee to cover the cost of verifying an 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.

Individuals not associated with the School as a student, parent, staff member or contractor can use a pseudonym or anonymously interact with the College. This situation is allowed where an individual is giving feedback or requesting publicly available information.

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, unless a student is aged 18 or over, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parent(s) or primary caregiver(s). The School will treat consent given by the parents as consent given on behalf of the student, and notice to parents will act as notice given to the student. A student who turns 18 years of age will be deemed to have consented or received notice on the same basis as his parents have consented or received notice prior to the student's 18th birthday, unless and until the student withdraws consent by giving notice to the School.

Parents may seek access to personal information held by the School about them or their child by contacting the Privacy Officer. However, there will be occasions when access is denied. Such occasions would include where release

of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student or an order of a court.

The School may, at its discretion, on the request of a student permit a 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.

Cross-Border Disclosure

As at the date of this Privacy Policy, the School is not likely to disclose personal information to any overseas recipients. If in future it does propose to disclose personal information overseas, the School will do so in compliance with the requirements of the Act and will, where practicable, advise affected individuals of the countries in which any overseas recipients are likely to be located.

By providing personal information to us, individuals consent to us disclosing their personal information to any such overseas recipients for purposes necessary or useful in the course of operating our business, and agree that Australian Privacy Principle 8.1 will not apply to such disclosures. For the avoidance of doubt, in the event that an overseas recipient breaches the Australian Privacy Principles, that entity will not be bound by, and you will not be able seek redress under, the Act.

If individuals do not want the School to disclose your information to overseas recipients, please let us know.

Complaints

If a person has concerns or complaints regarding the handling of their personal information, these concerns or complaints can be raised, in writing, with the Privacy Officer.

Complaints will be dealt with in an efficient and fair manner.

MANDATORY BREACH NOTIFICATION

Mandatory Breach Notification

The Privacy Amendment (Notifiable Data Breaches) Act 2017 requires St Peter's College, to undertake mandatory data breach notification to the Information Commissioner and any individuals affected by a data breach that is likely to result in serious harm.

For more detailed guidance, refer to https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

Where staff identify a suspected data breach, notification of the breach to the Director of Finance & Administration is required ASAP. Upon initial investigation, where it is believed St Peter's College has experienced or is involved in a data breach involving personal information held regarding external or internal people (over-and-above employee records), there are **four** key steps St Peter's College must follow to respond to and report a breach or suspected breach.

Refer to Appendix C for the detailed steps.

COMMUNICATION:

POLICY HISTORY:

Enquiries

Further information about the way the School manages the personal information it holds can be obtained by contacting the Privacy Officer (Director of Finance and Administration).

This Policy will be promulgated by the Headmaster and can be accessed via the School's website and its Information System – Keystone.

HISTORY	
Date Approved	**Amendments made (summary of major changes)**
July 2010	June 2013 (to bring in line with amendments to Privacy Act – March 2014)
Updates approved by SLT	February 2014 (to bring in line with amendments to Privacy Act – March 2014)
	April 2014 (to bring in line with amendments to Privacy Act – March 2014)
	June 2014 (to include that photographs are identified as personal information).
	February 2015 – updates made as per recommendations from Child Protection Desk Audit November 2014
	February 2018 – Updated to include information regarding Mandatory Breach Notification
	November 2019 – Updated to include information associated with the introduction of a digital facial recognition system

Appendix A – Written Collection statement script

Privacy Collection Statement
St Peter's College (SPC) is committed to the protection of your personal information and handling of that information in accordance with the Australian Privacy Principles and the Privacy Act 1988 (Cth) (Privacy Act).

SPC may collect personal information about you in the course of providing you with products or services. This personal information generally includes your name, contact information, date of birth and payment details. It may also include sensitive information including health information and biometric information or biometric templates. SPC generally collects personal information directly from you or, in the case of students, your parent or guardian, however some personal information may be collected using technological means or from other sources as specified in our Privacy Policy.

SPC will collect, use and disclose your personal information for the purposes of providing you with products and services, and for other purposes specified in our Privacy Policy. SPC usually discloses information such as your personal information to its associated entities, its contractors and advisors and the School community, and as otherwise specified in our Privacy Policy.

If SPC does not collect some or all of this personal information, we may not be able to provide you with some or all of our products or services.

Our Privacy Policy contains information about how you may access personal information about you that SPC holds and seek correction of such information, and about how you may complain about a breach of the Australian Privacy Principles and how SPC will deal with such a complaint.

SPC will not disclose personal information to overseas recipients. However, if SPC does disclose personal information to overseas recipients, it will do so in compliance with the Privacy Act. SPC's Privacy Officer (Director of Finance and Administration) can be contacted in relation to how SPC handles personal information, by contacting Reception.

Appendix B – Verbal Collection statement script

Verbal Privacy Collection Statement
When St Peter's College staff collect personal information, the following statement should be made:

"*The information we collect from you will be used for the purpose which we are discussing today. We handle your information according to our Privacy Policy, which is available on our website.*"

Appendix C – Mandatory Breach Notification Detailed Steps (refer to Appendix E for a short form checklist and flowchart)

Step 1: Contain the breach and do a preliminary assessment
Immediate steps: Initially, St Peter's College will take whatever steps possible to immediately contain the breach. This may include: stopping the unauthorised practice, recovering records, or shutting down (or limiting access) the system that was breached. Other actions include for example, if it is detected that a credit card number has been compromised, the affected individual and bank should be contacted to restrict further impact. Care is taken not to destroy evidence that may be valuable in determining the cause or would assist in appropriate corrective action.

Initial Assessment: St Peter's College's Director of Finance & Administration will lead the initial assessment to gather information and make initial recommendations. The initial assessment should include identifying details of personal information breached, causes, extent, impacts and how to contain from continuing. There is potential to engage 3rd party experts where complex breaches have occurred (for example forensic accountants, technology data experts or public relations). St Peter's College will take all reasonable steps to ensure that this assessment is completed within 30 days of becoming aware of a possible breach.

Communication: Determine who needs to be made aware of the breach (internally (which may include the Senior Leadership Team and the Emergency Committee of Council of Governors), and potentially externally), including notifying the affected individuals or report the breach to relevant internal investigation units or police if suspected theft or criminal activity. Other external parties are included in *Appendix C*.

Step 2: Evaluate the risks associated with the breach – is there an "eligible data breach"
This step will be led by St Peter's College Director of Finance & Administration and will consider the following factors in assessing the risks:

1. Determine the ***type of personal information*** involved: Physical, financial or psychological harm needs to be considered – Note:
    - a combination of personal information typically creates a greater risk of harm than a single piece of personal information
    - Permanent information, such as someone's name place and date of birth, or medical history cannot be 're-issued'
    - Consider who has been impacted: Employees, contractors, the public, clients, service providers, government agencies, organisations
2. Determine the ***context*** of the affected information and the breach: in particular, the *sensitivity* level of the information needs to be considered and how the impact changes because of the association with St Peter's College. Additionally:
    - Consider who or what parties have gained access to the information
    - Have there been other breaches that could have a cumulative effect?
    - How could the personal information be used (or combined with other information)?
3. Determine the ***cause and extent*** of the breach, and consider:
    - Is this a systemic problem or an isolated incident?
    - What was the source of the breach? (the risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious)
    - Is the personal information adequately encrypted, anonymised or otherwise not easily accessible?
    - What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
    - Is there evidence of theft?
    - Has the personal information been recovered?
    - How many individuals are affected by the breach?
4. ***Assess the risk*** of serious harm to the **affected individuals**, and consider:
    - Is there likely to be any relationship between the unauthorised recipients and the affected individuals?
    - What harm to individuals could result from the breach?:
        - 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.
5. Assess the ***risk of other harms*** and consider other possible harms, including:
        - the loss of public trust in St Peter's College

- reputational damage
- loss of assets (e.g., stolen computers or storage devices)
- 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.

Step 3: Notification
St Peter's College will consider the particular circumstances of the breach based on the previous analysis in Step 1 and 2, and:

1. ***decide whether to notify*** affected individuals, considering:
   - The key consideration is whether notification is necessary to avoid or mitigate serious harm to an affected individual.
   - What is the ability of the individual to avoid or mitigate possible harm if notified of a breach?
   - Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
   - What are the legal and contractual obligations to notify, and what are the consequences of notification?

   and, if so:
2. consider ***when*** (generally asap, with law enforcement if required) and ***how*** (generally **direct)** notification should occur, ***who*** should ***make*** the notification, and ***who should be notified***
3. consider ***what information*** should be included in the notification (*refer to Appendix D*), and
4. consider ***who else*** (other than the affected individuals) should be notified (*refer Appendix D*).

In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified as soon as practicable

Step 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, St Peter's College will investigate the cause and consider whether to develop a prevention plan.

This plan may include:

- a security audit of both physical and technical security
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that
- a review of employee selection and training practices, and
- a review of service delivery partners (for example, offsite data storage providers).

Other considerations include:

Appendix D – Breach Notification Guide

- the creation of a senior position in with specific responsibility for data security
- the institution of a ban on bulk transfers of data onto removable media without adequate security protection (such as encryption)
- disabling the download function on computers in use, to prevent the download of data onto removable media
- the institution of a ban on the removal of unencrypted laptops and other portable devices from St Peter's College sites
- the institution of a policy requiring the erasing of hard disk drives and other digital storage media (including digital storage integrated in other devices such as multifunction printers or photocopiers) prior to being disposed of or returning to the equipment lessor
- the use of secure couriers and appropriate tamper proof packaging when transporting bulk data, and
- the upgrading of passwords (for example, an increase from 6 to 8 characters, including numbers and punctuation), and the institution of a policy requiring passwords to be changed every 8 weeks.

Breach Notification Guide

1. Notifications should include the types of information detailed below:

- Incident Description — Information about the incident and its timing in general terms
- Type of personal information involved — A description of the type of personal information involved in the breach
- Response to the breach — A general account of what St Peter's College has done to control or reduce the harm and proposed future steps that are planned.
- Assistance offered to affected individuals — What St Peter's College will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves.
- Other information sources — Sources of information designed to assist individuals in protecting against identity theft or interferences with privacy.
- St Peter's College contact details
- Whether breach notified to regulator or other external contact(s) (refer below)
- Legal implications — St Peter's College should consider whether to seek legal advice
- How individuals can lodge a complaint St Peter's College – *We request that individuals or organisations first make a complaint in writing. We will confirm receipt of the complaint and it will be investigated and St Peter's College will respond to within a reasonable time. Where the individual or organisation is not satisfied with the handling of your complaint, they may contact the Office of the Australian Information Commissioner with your complaint (below)*
- How individuals can lodge a complaint with the OAIC – contact details are:

  The Office of the Australian Information Commissioner

  GPO Box 2999
  Canberra ACT 2601

Phone: 1300 363 992
Fax: (02) 9284 9666
Website: www.oaic.gov.au

- How individuals can lodge a complaint with the SA privacy regulator —

  State Records, South Australia

  GPO Box 2343
  Adelaide SA 5001
  Phone (08) 8204 8786
  Fax: (08) 8204 8777
  Email: privacy@sa.gov.au
  Website: www.archives.sa.gov.au/privacy/index.html

2. Who else should be notified?

In general, notifying the OAIC, or other authorities or regulators should not be a substitute for notifying affected individuals. However, in some circumstances it may be appropriate to notify these third parties:

- **OAIC** — Report serious data breaches to the OAIC. The following factors should be considered in deciding whether to report a breach to the OAIC:
  - any applicable legislation that may require notification
  - the type of the personal information involved and whether there is a **real risk of serious harm** arising from the breach, including non-monetary losses
  - whether a large number of people were affected by the breach
  - whether the information was fully recovered without further disclosure
  - whether the affected individuals have been notified, and
  - if there is a reasonable expectation that the OAIC may receive complaints or inquiries about the breach.
- **Police** — If theft or other crime is suspected. The Australian Federal Police should also be contacted if the breach may constitute a threat to national security.
- **Insurers** or others — If required by contractual obligations.
- **Credit card companies, financial institutions or credit reporting agencies** — If their assistance is necessary for contacting individuals or assisting with mitigating harm.
- **Professional or other regulatory** bodies — If professional or regulatory standards require notification of these bodies. For example, other regulatory bodies, such as the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission, and the Australian Communications and Media Authority have their own requirements in the event of a breach.
- **Other internal or external parties not already notified** — Consider the potential impact that the breach and notification to individuals may have on third parties and take action accordingly. For example, third parties may be affected if individuals cancel their credit cards, or if financial institutions issue new cards.
- Consider:
  - third party contractors or other parties who may be affected

  - internal business units not previously advised of the breach, (for example, communications and media relations, senior management), or
  - union or other employee representatives.
- Government Agencies that have a direct relationship with the information lost/stolen — Consider whether an incident compromises Australian Government agency identifiers such as TFNs or Medicare numbers. Notifying agencies such as the Australian Taxation Office for TFNs or Medicare Australia for Medicare card numbers may enable those agencies to provide appropriate information and assistance to affected individuals, and to take steps to protect the integrity of identifiers that may be used in identity theft or other fraud.

Appendix E – short form Mandatory Breach Reporting checklist

Breach Event: Date:	
Step	**Completed?**
Step 1: Contain the breach and do a preliminary assessment	
***Immediate steps**:* Contain the breach.	
***Initial Assessment**:* Gather information and make initial recommendations.	
***Communication**:* Determine who needs to be made aware of the breach.	
Step 2: Evaluate the risks associated with the breach	
Determine the:	
• ***type of personal information*** involved:	
• ***context*** and the *sensitivity* level of the information	
• ***cause and extent*** of the breach	
• Then: ***Assess the risk*** of serious harm to the **affected individuals**.	
• Assess the ***risk of other harms***	
Step 3: Notification	
• ***decide whether to notify*** affected individuals.	
• consider ***when*** (generally asap, with law enforcement if required) and ***how*** (generally **direct)** notification should occur, ***who*** should ***make*** the notification, and ***who should be notified.***	
• consider ***what information*** should be included in the notification.	
• consider ***who else*** (other than the affected individuals) should be notified.	
Step 4: Prevent future breaches	
Develop a prevention plan:	
This plan may include:	
• a security audit of both physical and technical security	
• a review of policies and procedures and any changes to reflect the lessons learned from the investigation	
• a review of employee selection and training practices, and	
• a review of service delivery partners (for example, offsite data storage providers).	

Mandatory Data Breach Reporting Flowchart

Mandatory%20Data
%20Breach%20Repc