PRIVACY POLICY & OBLIGATIONS

St Lucy's School is an independent Catholic Special School which is part of Dominican Education Australia (DEA). St Lucy's provides for children with a wide range of disabilities.

Purpose: This Privacy Policy informs individuals about the practices of the School in relation to personal information. It also serves as a guide to the School's staff as to the standards to be applied in respect of handling personal information and ensure consistency in the School's approach to privacy.

Refer to collection notices, to satisfy the requirements in APP 5.2 to ensure that individuals are aware of relevant matters on collection of personal information.

Overview: This Privacy Policy sets out how the School manages personal information provided to or collected by it. The School is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act 1988. In relation to health records, the School is also bound by the Health Privacy Principles which are contained in the Health Records and Information Privacy Act 2002 (NSW) (Health Records Act).

The School may, from time to time, review and update this Privacy Policy 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.

Policy:

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 health and other sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the School, including:
- name, contact details (including next of kin), date of birth, gender, language
- background, previous school and religion;
- parents' education, occupation and language background;
- medical information (e.g. details of disability and/or allergies, absence notes,

- medical reports and names of doctors);
- conduct and complaint records, or other behaviour notes, and school reports;
- information about referrals to government welfare agencies;
- counselling reports;
- health fund details and Medicare number;
- any court orders;
- volunteering information; and
- photos and videos at School events;
- information about relevant specialists and specialist reports/assessments
- relevant psychometric assessments and specialist reports – identify disability information and functioning;

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);
- medicine taking for camp forms
- complaint records and investigation reports;
- leave details;
- photos and videos at School events;
- workplace surveillance information;
- work emails and private emails (when using work email address) and Internet
- browsing history; and
- other people who come into contact with the School, including name and contact details and any other information necessary for the particular contact with the School.

Personal Information you provide: The School will generally collect personal information held about an individual by way of forms filled out by Parents or pupils, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than Parents and pupils provide personal information.

Personal Information provided by other people: 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.

Exception in relation to employee records: Under the Privacy Act and the Health Records Act, the Australian Privacy Principles and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does 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.

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.

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

The purposes for which the School uses personal information of pupils 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 pupils' 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 pupil or Parent, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the pupil or permit the pupil 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 pupils 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 or, on occasions, external fundraising organisations. Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes, using first name only unless express permission from Parents.

Photos taken of children during school events on any personal device i.e. camera or phones must be uploaded onto school server and removed from the personal device within 3 days

Retention of Confidential Information:

In applying for a vacant position, St Lucy's is provided with personal information. For example, name and address or information contained on cover letter and curriculum vitae. St Lucy will collect the information in order to assess application for employment.

St Lucy's will keep cover letters and curriculum vitae on file. If the applicant is unsuccessful the cover letter and curriculum vitae will be kept for a period of two years, in the event that another position becomes available. All other information will be destroyed. Should applicants wish to have information destroyed earlier, notification required to Executive Assistant.

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 (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, coaches, volunteers, and counsellors;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);

- people providing administrative and financial services to the School;
- recipients of School publications, such as newsletters and magazines; pupils' 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 (in some cases this consent will be implied); 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.

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, trade union or other professional or trade association membership, philosophical beliefs, disability, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

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

Management and security of personal information

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

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.

Access and correction of personal information

Under the Commonwealth Privacy Act and the Health Records 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. (Primary aged children will generally be able to access and update their personal information through their Parents, but older pupils 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 Principal 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 pupils

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 pupil to the pupil's Parents. The School will treat consent given by Parents as consent given on behalf of the pupil, and notice to Parents will act as notice given to the pupil.

Parents may seek access to personal information held by the School about them or their child by contacting the School 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 pupil.

The School may, at its discretion, on the request of a pupil grant that pupil access to information held by the School about them, or allow a pupil 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 pupil and/or the pupil's personal circumstances warrant it.

Enquiries and complaints

If you would like further information about the way the School 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 School Principal in writing. The School will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

Date Approved/Reviewed	August 2020
Approval Authority	School Principal
Date for Next Review	August 2022

ANNEXURE 1 – SUMMARY OF A SCHOOL'S OBLIGATIONS

IMPOSED BY THE AUSTRALIAN PRIVACY PRINCIPLES

1. Manage personal information in an open and transparent way.
2. Take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the School's functions or activities that:
   a) will ensure compliance with the APPs; and
   b) will enable the School to deal with inquiries or complaints about compliance with the APPs.
3. Have a clearly expressed and up-to-date Privacy Policy about the School's management of personal information.
4. If it is lawful or practicable, give individuals the option of interacting anonymously with the School or using a pseudonym.
5. Only collect personal information that is reasonably necessary for the School's functions or activities.
6. Obtain consent to collect sensitive information unless specified exemptions apply.
7. Use fair and lawful means to collect personal information.
8. Collect personal information directly from an individual if it is reasonable and practicable to do so.
9. If the School receives unsolicited personal information, determine whether it could have collected the information under APP 3 as if it had solicited the information. If so, APPs 5-13 will apply. If not, the information must be destroyed or de-identified.
10. At the time the School collects personal information or as soon as practicable afterwards,take such steps (if any) as are reasonable in the circumstances to make an individual aware of:
    a) why the School is collecting information about them;
    b) who else the School might give it to; and
    c) other specified matters.
11. Take such steps (if any) as are reasonable in the circumstances to ensure the individual is aware of this information even if the School has collected it from someone else.
12. Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in APP 6.2 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances).
13. If the information is sensitive, the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the primary purpose of collection.
14. Do not use personal information for direct marketing, unless one of the exceptions in APP 7 applies (for example, the School has obtained consent or where the individual has a reasonable expectation of their information being used or disclosed for that purpose and the School has provided a simple means for the individual to unsubscribe from such communications).
15. Before the School discloses personal information to an overseas recipient it must take such steps as are reasonable in the circumstances to ensure that the recipient does not breach the APPs, unless an exception applies.
16. Government related identifiers must not be adopted, used or disclosed unless one of the exceptions applies (eg. the use or disclosure is reasonably necessary to verify the identity of the individual for the purposes of the School's functions or activities).
17. Take such steps (if any) as are reasonable in the circumstances to ensure the personal information the School collects, uses or discloses is accurate, complete and up-to-date. This may require the School to correct the information and possibly advise organisations to whom it has disclosed the information of the correction.
18. Take such steps as are reasonable in the circumstances to protect the personal information the School holds from misuse, interference and loss and from unauthorised access, modification or disclosure.

19. Take such steps as are reasonable in the circumstances to destroy or permanently de identify personal information no longer needed for any purpose for which the School may use or disclose the information.
20. If requested, the School must give access to the personal information it holds about an individual unless particular circumstances apply that allow it to limit the extent to which it gives access

Note: This is a summary only and **NOT** a full statement of obligations

ANNEXURE 2 – MANDATORY NOTIFICATION OF ELIGIBLE DATA BREACHES SUMMARY

Schools have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known Data Breach

Possible

Assess

Schools will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the School has reasonable grounds to believe this is the case, then this is an EDB and it must notify individuals affected and the Information Commissioner. If it only has grounds to suspect that this is the case, then it must conduct an assessment. As part of the assessment, Schools should consider whether remedial action is possible.

Schools should consider adopting the OAIC's suggested a three-stage process: Initiate: plan the assessment and assign a response team or person Investigate: gather relevant information about the incident to determine what has occurred. Evaluate: make an evidence-based decision about whether serious harm is likely (and document this).Schools should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, a School should take steps to reduce any potential harm to individuals. For example, this might involve taking action to recover lost information before it is accessed or changing access controls on accounts before unauthorised transactions can occur. If remedial action is successful in making serious harm no longer likely, then notification is not required and Schools can progress to the review stage

NO **Is serious harm still likely?** **YES**

Notify

Where **serious harm is likely**, a School must prepare a statement for the Commissioner (a form available on OAIC website) that contains:

the School's identity and contact details
a description of the Data Breach
- the kind/s of information concerned
- recommended steps for individuals affected

Schools must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:**Option 1:** Notify all individuals **Option 2:** Notify only those individuals at risk of serious harm . If neither of these options are practicable: **Option 3:** publish the statement on the School's websiteand publicise it

Schools can provide further information in their notification, such as an apology and an explanation of what they are doing about the Data Breach. **In some limited circumstances, an exception to the obligation to notify the individuals or the Commissioner may apply**

Review

Review the incident and take action to

prevent future Data Breaches. This may include:

Fully investigating the cause of the Data Breach
Developing a prevention plan
Conducting audits
Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Schools should also consider reporting the incident to other relevant bodies, such as:

police or law enforcement
other external or third parties (eg the ATO)
The Australian Cyber Security Centre and related agencies
professional bodies
Credit card companies or financial services providers
Schools that operate outside Australia may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation

ANNEXURE 3 – DATA BREACH RISK ASSESSMENT FACTORS

Consider who the personal information is about

Who is affected by the breach? Are pupils, parents, staff, contractors, service providers, and/or other agencies or organisations affected?

For example, a disclosure of a pupil's personal information is likely to pose a greater risk of harm than a contractor's personal information associated with the contractor's business.

Consider the kind or kinds 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.

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 pupils who attend the School may not give rise to significant risk. However, the same information about pupils who have attended the School counsellor or students with disabilities may be more likely to cause harm. The disclosure of names and address of pupils 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 pupil's name, address and grades without malicious intent (eg if the information is accidentally emailed to the teacher), the risk of serious harm to the pupil 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 is considered. This could involve incremental breaches of the same School database, or known breaches from multiple different sources (eg 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 pupils' domestic circumstances may be used to bully or marginalise the pupil 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?

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 of the breach?For example, was it external or internal? Was it malicious or unintentional? Did it 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 affec**ted individuals.**

Who is the information about? Some individuals are more vulnerable and less able to take steps to protect themselves (e.g. younger students, students with disabilities/special needs, vulnerable families/parents)

What kind or kinds 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 pupils who attend the School may not be sensitive information. However, the same information about pupils 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 pupil number that only the School uses – this should be contrasted to a pupil 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 likelihood that any of those security measures could be overcome? For example, could an attacker have overcome network security measures protecting personal information stored on the network?

What persons (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 who may wish to cause harm to the individual to whom the information relates. For instance, if a teacher gains unauthorised access to a pupil's information without malicious intent, the risk of serious harm may be unlikely.

What is the nature of the harm that could result from the breach? Examples include identity theft, financial loss, threat to physical safety, threat to emotional wellbeing, loss of business or employment opportunities, humiliation, damage to reputation or relationships, or workplace or social bullying or marginalisation. For example, information on pupils' 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 remediate the serious harm to affected individuals might include promptly resetting all user passwords, stopping an unauthorised practice, recovering records subject to unauthorised access or disclosure or loss, shutting down a system that was subject to unauthorised access or disclosure, or remotely erasing the memory of a lost or stolen device. Considerations about how quickly these steps are taken or the extent to which the steps taken are remediating harm will vary depending on the circumstances.

Any other relevant matters?The nature of other matters that may be relevant will vary depending on the circumstances of the School and the Data Breach.

Assess the risk of other harms.

What other possible harms could result from the breach, including harms to the School or AIS/CEC? Examples include loss of public trust in the School or AIS/CEC, damage to reputation, loss of assets (e.g. stolen laptops), financial exposure (e.g., if bank account details are compromised), regulatory penalties (e.g., for breaches of the Privacy Act), extortion, legal liability, and breach of secrecy provisions in applicable legislation.

ANNEXURE 4 – TEMPLATE DATA BREACH RESPONSE PLAN

Introduction

The template plan sets out the procedure to manage a School's response to the actual or suspected unauthorised access to or disclosure or loss of personal information (Data Breach). The School will need to adapt this template to their circumstances and may also wish to seek guidance from the Catholic Education Office, the Catholic Education Commission, or the Association of Independent Schools to which they belong. Further guidance about responding to a Data Breach and an eligible data breach (EDB) under the notifiable data breaches scheme (NDB Scheme) is contained in Section 26.

Response plan

In the event of a Data Breach, School personnel must adhere to the four phase process set out below (as described in the Office of the Australian Information Commissioner's (OAIC) Notifiable Data Breaches scheme: Resources for agencies and organisations. It is important that appropriate records and any evidence are kept of the Data Breach and the response. Legal advice should also be sought if necessary.

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

1. The School personnel who becomes aware of the Data Breach or suspects a Data Breach has occurred must immediately notify The Principal or Deputy Principal. That person must take any immediately available steps to identify and contain the Data Breach and consider if there are any other steps that can be taken immediately to mitigate or remediate the harm any individual could suffer from the Data Breach.

2. In containing the Data Breach, evidence should be preserved that may be valuable in determining its cause.

3. The Principal or Deputy Principal must make a preliminary assessment of the risk level of the Data Breach. The following table sets out examples of the different risk levels.

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 Risk Data Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

4. Where a **High Risk** incident is identified, David Raphael, Principal or Susan Jones Deputy Principal must consider if any of the affected individuals should be notified immediately where serious harm is likely.

5. David Raphael, Principal or Susan Jones Deputy Principal must escalate High Risk and Medium Risk Data Breaches to the response team (whose details are set out at the end of this protocol).

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

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

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

2. The response team is to work to evaluate the risks associated with the Data Breach, including by:

a. identifying the type of personal information involved in the Data Breach;

b. identifying the date, time, duration, and location of the Data Breach;

c. establishing who could have access to the personal information;

d. establishing the number of individuals affected; and

e. establishing who the affected, or possibly affected, individuals are.

3. The response team must then assess whether the Data Breach is likely to cause serious harm to any individual whose information is affected by the Data Breach, in which case it should be treated as an EDB.

4. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.

5. All reasonable steps must be taken to ensure that the assessment is completed as soon as possible and in any event within 30 days after they suspect there has been a Data Breach.

Phase 3. Consider Data Breach notifications

6. The response team must determine whether to notify relevant stakeholders of the Data Breach, including affected individuals, parents and the OAIC even if it is not strictly an EDB.

7. As soon as the response team knows that an EDB has occurred or is aware that there are reasonable grounds to believe that there has been an EDB, they must prepare a statement with the prescribed information and give a copy of the statement to the Information Commissioner.

8. After completing the statement, unless it is not practicable, the response team must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the EDB.

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

Phase 4. Take action to prevent future Data Breaches

10. 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.

11. The Principal or Deputy Principal must enter details of the Data Breach and response taken into a Data Breach log. [insert name of relevant person] must, every year, review the Data Breach log to identify any reoccurring Data Breaches.

12. The Principal or Deputy Principal must conduct a post-breach review to assess the effectiveness of the School's response to the Data Breach and the effectiveness of the Data Breach Response Protocol.

13. The Principal or Deputy Principal must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.

14. The Principal or Deputy Principal must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Data Breach and conduct an audit to ensure the plan is implemented.

Response Team

David Raphael, Principal	Davidr@stlucys.nsw.edu.au
Or	
Susan Jones Deputy Principal	susanj@stlucys.nsw.edu.au
Maria Manzatti, IT co-ordinator	mariam@stlucys.nsw.edu.au
Or	
Caroline Fowler, Business Manager	carolinef@stlucys.nsw.edu.au
Or	
Nicole Foxall, Finance & HR Officer	nicolef@stlucys.nsw.edu.au

ANNEXURE 5 - PRIVACY BREACH RESPONSE PROTOCOL

Introduction

This protocol sets out the procedure to manage St Lucy's response to an actual or suspected misuse, interference, loss or unauthorised access, modification or disclosure of personal information (Privacy Breach). It is intended to enable St Lucy's to contain, assess and respond to a Privacy Breach.

Response Protocol

In the event of a Privacy Breach, St Lucy's personnel must adhere to the following four (4) phase process guide. Phases 1 to 3 should occur in quick succession and may occur simultaneously.

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

Risk Table

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) has been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Privacy Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (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. 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.

7. 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.

8. 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)

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

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

11. 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 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 (e.g. 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;

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

6. 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) Office of the Australian Information Commissioner (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)

7. 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) and the OAIC should be notified.

8. The response team will facilitate ongoing discussion with the OAIC as required.

Phase 4: Take action to prevent future Privacy Breaches

9. 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.

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

11. The Privacy Officer 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.

12. The Privacy Officer must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating the Privacy Breach Response Protocol.

13. The Privacy Officer must, 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 Responsibilities & Authorities First Contact Person Second Contact Person

Role	Responsibilities & Authorities	First Contact Person	Second Contact Person
Principal	• Take immediate steps to contain the privacy breach. • Consider any steps that can be taken immediately to mitigate the harm an individual may suffer from the privacy breach. • Preliminary assessment of the risk level of the privacy beach. (High, Medium or Low Risk) • Escalate High & Medium Risk privacy breaches to the response team. • Low Risk privacy breaches are dealt with by the Principal.	Principal David Raphael Phone: 0422 007 311	Duty Principal Susan Jones Phone:0410 774 722
IT Department	• For High & Medium privacy breaches you will be engaged as a part of the response team to assist with the privacy breach. • Responsible for the shut-down of relevant systems or remove access to the system depending on the privacy breach.	IT Co-ordinator Maria Manzatti Phone:0414 359 639	APEK Phone:0421 997 996/9906 8228
Privacy Officer/Human Resources	• For High & Medium privacy breaches you will be engaged as a part of the response team to assist with the privacy breach. • Maintain a privacy breach log and carry out a post-breach review to assess the effectiveness of the response to the privacy breach.	Business Manager Caroline Fowler Phone: 0413 307 598	HR & Finance Officer Nicole Foxall Phone: 0402 116 886

Contacts

National Computer Emergency Response Team (CERT)

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

Office of the Australian Information Commissioner (OAIC)

Report Privacy Breaches to OAIC via email (enquiries@oaic.gov.au) or telephone (1300 363 992)