PRIVACY POLICY, PLAN AND BREACH PROCEDURES

CONTENTS

PRIVACY POLICY, PLAN AND BREACH PROCEDURE

RATIONALE

Holy Saviour School is committed to protecting the privacy of our stakeholders, including students, teachers, parents, carers, staff and members of the public. The School protects the personal and health information we hold in accordance with NSW privacy laws, the *Privacy and Personal Information Protection Act 1998* (PPIPA) and the *Health Records and Information Privacy Act 2002* (HRIPA), which require us to comply with Information and Health Privacy Principles.

POLICY

Holy Saviour School is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act 1988, articulated in this policy. 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). The health principles align to the twelve Australian Privacy Principles.

This Privacy Policy articulates how our School manages Personal and Health Information provided or collected by the School.

The information provided and collected are that of, employees, students and other stakeholder information including information about parents and carers and information obtained in the course of employment or education at Holy Saviour School.

The Policy, Plan and Procedures resonate the embedded NSW Child Safe Standards 1, 3, 4, 5, 6, 7, 8, 9 & 10.

DEFINITIONS

What is Personal Information? Personal information is any information about an individual who is identifiable. It could be a student's name, address, class, school, family details, fingerprints or a combination of information from which a student, employee or other individual can be identified. The information can be in recorded in paper files, electronic records, video recordings and photographs.

Personal information is defined as:

- Information or an opinion (including information or an opinion forming part of a database and
- whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Health information is defined as:

- Personal information that is information or an opinion about the physical, mental health or disability (at any time) of an individual.

Holy Saviour School implements the twelve Commonwealth privacy principles to protect the privacy of all members of the community and for the effective management and function of the School.

COMMONWEALTH PRIVACY PRINCIPLES

COLLECTION

1. Lawful: Holy Saviour School only collects personal information for a lawful purpose. It directly related to the School function or activities and necessary for that purpose.

2. Direct: Holy Saviour School only collects personal information directly from you, unless you have authorised collection from someone else, or if you are under the age of 16 and the information has been provided by a parent or guardian.

3. Open: The School will inform you that the information is being collected, why it is being collected, and who will be storing and using it. You must also be told how you can access and correct your personal information, if the information is required by law or is voluntary, and any consequences that may apply if you decide not to provide it.

4. Relevant: The School must ensure that your personal information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into your personal affairs.

STORAGE

5. Secure: The School will store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

ACCESS AND ACCURACY

6. Transparent: The School provides you with details regarding the personal information they are storing, why they are storing it and what rights you have to access it.

7. Accessible: An agency must allow you to access your personal information without excessive delay or expense.

8. Correct: An agency must allow you to update, correct or amend your personal information where necessary.

USEAGE

9. Accurate: The School must ensure that your personal information is relevant, accurate, up to date and complete before using it.

10. Limited: The School can only use your personal information for the purpose for which it was collected unless you have given consent, or the use is directly related to a purpose that you would expect, or to prevent or lessen a serious or imminent threat to any person's health or safety.

DISCLOSURE

11. Restricted: An agency can only disclose your information in limited circumstances if you have consented or if you were told at the time, they collected it that they would do so. An agency can also disclose your information if it is for a directly related purpose and it can be reasonably assumed that you would not object, if you have been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded: An agency cannot disclose your sensitive personal information without your consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

PRIVACY PLAN

When collecting personal information, Holy Saviour School will take reasonable steps to ensure that the person to whom it relates is made aware of certain matters including the purpose for which it is being collected, the intended recipients of the information and the person's right to access and correct the information.

This Privacy Plan articulates the context and type of information collected and held by the School under the headings of the Australian Privacy Principles. The plan has the embedded implement of the NSW Child Safe Standards 1, 3, 4, 5, 6, 7, 8 and 10.

COLLECTION

The information the School collects and holds includes (however, not limited to) personal information, including health and other sensitive information.

Collection of Students and parents and/or guardians ('Parents') information before, during and after a pupil's enrolment at the School, includes:

- Name, contact details (including next of kin), date of birth, gender, language background, previous school and religion
- Parent's education, occupation and language background.
- Medical information (e.g., details of disability and/or allergies, absence notes, medical reports and names of doctors)

- Results of assignments, tests and examinations
- 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
- Court orders
- Volunteering information; and
- photos and videos at School events.

Job applicants, staff members, volunteers and contractors, including:

- Name, contact details (including next of kin), date of birth, and religion
- Information on job application
- Professional development history
- Salary and payment information, including superannuation details
- Medical information (e.g., details of disability and/or allergies, and medical certificates).
- Complaint records and investigation reports
- Leave details
- Photos and videos at School events
- Workplace surveillance information
- Work emails and private emails (when using work email address) and Internet browsing history

PERSONAL INFORMATION YOU PROVIDE: The School will generally collect personal information held about an individual by way of forms, face-to-face meetings and interviews, emails and telephone calls. On occasions people other than parents, pupils and staff 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.

USAGE: 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 that to which is reasonably expected, or to which you have consented.

1. 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 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 student and the needs of the School throughout the whole period the student is enrolled at the School.

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

- To keep parents informed about matters related to their child's schooling, through

correspondence, newsletters and magazines

- Day-to-day administration
- Looking after pupils' educational, social, and medical wellbeing
- Seeking donations and marketing for the School
- To satisfy the School's legal obligations and allow the School to discharge its duty of care
- In some cases, where the School requests personal information about a student or parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

2. 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:

(a) Administering the individual's employment or contract, as the case may be for insurance purposes

(b) Seeking donations and marketing for the School

(c) Satisfying the School's legal obligations, for example, in relation to child protection legislation.

3. Volunteers:

The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as P&F associations, to enable the School and the volunteers to work together.

4. 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 may be disclosed to organisations that assist in the fundraising, for example, the Schools P&F Association 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 and maybe used for marketing purposes.

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

This may include:

- Other Schools and teachers at those Schools
- Government departments (including for policy and funding purposes)
- The School's local parish
- Medical practitioners
- People providing educational, support and health services to the School, including specialist
- visiting teachers, sports coaches, volunteers, counsellors
- Providers of specialist advisory services and assistance to the School, including in the area of
- Human Resources, child protection and students with additional needs
- 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
- Agencies and organisations to whom we are required to disclose personal information for
- education, funding and research purposes
- People providing administrative and financial services to the School
- Recipients of School publications, such as newsletters and magazines
- Students' parents or guardians
- Anyone you authorise the School to disclose information to
- 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 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. This 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 providers server which may be situated outside Australia.

SENSITIVE INFORMATION: In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; 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: Holy Saviour School members are required to respect the confidentiality of individual staff, students and Parents' personal information and their privacy. All staff read, understand and sign an acknowledgment complying with the Privacy Policy, Plan and Breach Procedure.

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 ACCURACY: 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. Students will generally be able to access and update their personal information through their parents, but older students may seek access and correction themselves.

There are some exceptions to this right, set out in the applicable legislation. To make a request to access or to update any personal information the School holds about you or your child, please contact the School Administration by telephone or in writing. The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal (unless, in the light of the grounds of refusing, it would be unreasonable to provide reasons).

Content and Right of Assess to Personal Information of STUDENTS

The School respects every parent's right to make decisions concerning their child's education. Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents. The School will treat consent given by parents as consent given on behalf of the student and notice to parents will act as notice given to the student. Parents may seek access to personal information held by the School about them or their child by contacting the School Administration by telephone or in writing.

However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

The School may, at its discretion, on the request of a student grant that student access to information held by the School about them or allow a student to give or withhold consent to the use of their personal information, independently of their parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances warrant it.

COMPLAINTS

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.

See the School's 'Privacy Breach Protocols and Procedures' in this document.

ENQUIRIES

If you would like further information about the way the School manages the personal information

it holds, please contact the Administration Office.

Email: Info@holysaviour.nsw.edu.au

PRIVACY BREACH PROTOCOLS AND PROCEDURES

INTRODUCTION

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

RESPONSE PROTOCOL

In the event of a Privacy Breach, the School personnel must adhere to the following four phase process (as described in the Office of the Australian Information Commissioner's (OAIC) guide Data breach notification: a guide to handling personal information security breaches).

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

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

PHASE 1: Contain the Privacy Breach and Preliminary Assessment

1. The School personnel who become 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 Finance Manager, 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 a preliminary assessment of the risk level of the Privacy Breach. This will involve an analysis of the risks involved. The following table sets out examples of the different risk levels.

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 Privacy Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and 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, she may determine that the response team does not need to be convened. In this case, she must undertake Phases 2 and 3 below.
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 Risks Associated with the Privacy Breach

1. The response team is to take any further steps (i.e., those not identified in Phase 1) available to contain the Privacy Breach and mitigate harm to affected individuals.
2. The response team is to work to evaluate the risks associated with the Privacy Breach by:

   (a) identifying the type of personal information involved in the Privacy Breach.
   (b) Identifying the date, time, duration, and location of the Privacy Breach.
   (c) Establishing the extent of the Privacy Breach (number of individuals affected).
   (d) Establishing who the affected, or possibly affected, individuals are.
   (e) identifying what is the risk of harm to the individual/s and the extent of the likely harm (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 College and CSNSW.
   (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: Privacy Breach Notifications

1. Where appropriate, having regard to the seriousness of the Privacy Breach (based on the evaluation above), the response team must determine whether to notify the following stakeholders of the Privacy Breach:
   - Affected individuals.
   - Parents
   - The OAIC; and/or
   - Other stakeholders (e.g., if information which has been modified without authorisation is disclosed to another entity, that entity may need to be notified).
2. In general, if a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals (and their parents if the affected individuals are pupils) the OAIC will be notified.

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

PHASE 4: Action to Prevent Future Privacy Breaches

1. The response team must complete any steps in phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3. The cause of the Privacy Breach must be fully investigated.
2. The Finance Manager must enter details of the Privacy Breach and response taken into a Privacy Breach log. The Finance Manager every year, will review the Privacy Breach log to identify any reoccurring Privacy Breaches.
3. The Finance Manager 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.
4. The Finance Manager in conjunction with members of the Executive team must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Privacy Breach Response Protocol.
5. The Finance Manager in conjunction with members of the Executive team 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 and authorities	First contact person	Second contact person
Principal	Responsible for Leadership in guiding the School to better teaching and learning Responsible for communicating with the Finance Manager and ICT Consultant.	Ms Dianne Klumpp	Ms Rachael Bryant
Finance Manager	Responsible for Business Financial, Operational and Administration functions of the school. Responsible for communicating with the Principal and ICT Consultant	Mr Gavin Carolan	Pamela Aboud
Assistant Principal	Leverage existing media relationships and cultivate new contacts within the Education sector, School community and media.	Rachael Bryant	Sue Nabaaki
Compliance and HR Manager	Ensure functional link between the School and CSNSW/SISNSW	Dianne Klumpp	Rachael Bryant

REFERENCES

- Privacy Compliance Manual November 2019
- Commonwealth Privacy Act 1988.
- Health Records and Information Privacy Act 2002 (NSW)
- OAIC's Data breach notification: a guide to handling personal information security breaches
- OAIC's Guide to developing a data breach response plan
- OAIC's website at www.oaic.gov.au

RELATED DOCUMENTATION

- Staff Code of Conduct Policy
- Complaints Handling Policy and procedures
- Child Protection Policy and Procedures

USEFUL CONTACTS

National Computer Emergency Response Team (CERT)

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

Office of the Australian Information Commissioner (OAIC)

Report Privacy Breaches to OAIC via email (enquires@oaic.gov.au) or telephone 1300 3

POLICY Dates			
Implementation	August 2013	Reviewed	July, 2015, Feb, 2017, Oct 2018, 9th Aug,2023
Next Policy Review Date	August, 2027		
Policy Authorisation	Principal: Dianne Klumpp		
Policy Number	0003		

This Policy and its procedures supersede all previous policies and procedures relating to the matters contained herein.

PRIVACY POLICY, PLAN and BREACH PROCEDURE

Acknowledgement

I _____ (full name) have read, understand, and agree to comply with the terms of Holy Saviour School's Privacy Policy, Plan and Breach Procedures Documents.

Position: _____

Signed: _____ Date: _____