Stella Maris
COLLEGE MANLY

Privacy Policy

a 52 Eurobin Avenue, Manly NSW 2095 t +61 2 9977 5144 f +61 2 9976 2753 cricos 03290E
e administration@stellamaris.nsw.edu.au w www.stellamaris.nsw.edu.au abn 88 058 323 827

PREAMBLE

Stella Maris College (the College) is a school of Good Samaritan Education established in 1931 in the Benedictine tradition. The policies of the College give expression to its values and ethos and/or reflect the legal requirements of a school registered and accredited by the NSW Education Standards Authority (NESA).

POLICY

Stella Maris College is bound by the Australian Privacy Principles contained in the *Commonwealth Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012*. In relation to health records the College is also bound by the *Health Records and Information Privacy Act 2002*.

The primary purpose of collecting personal information about students and their parents/carers is to enable the College to provide appropriate educational opportunities for its students, to satisfy legal obligations and to facilitate the College's duty of care. Enrolment is contingent upon receipt of such information.

The primary purpose of collecting personal information from job applicants, staff members and contractors is to assess and (if successful) to engage the applicant, staff member or contractor. Information will be used to administer the individual's employment or contract, for insurance purposes and to satisfy legal obligations.

This policy does not apply to employee records directly related to the employment relationship.

The primary purpose of collecting personal information from volunteers and others is to facilitate a working partnership between the individual and the College and for legal obligations.

The College collects personal information, including sensitive and health information about:
- Students and parents/carers before, during and after the course of a student's enrolment at the College.
- Employment applicants, staff members, volunteers and contractors.
- Other people who come into contact with the College.

The kinds of personal information the College collects, and how it is collected, is largely dependent upon whose information is being collected and why we are collecting it, however, in general terms the College may collect:
- Personal Information – including names, addresses and other contact details, dates of birth, next of kin details, financial information, photographic images and attendance records.
- Sensitive Information – including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional membership, family court orders and criminal records.
- Health Information – including medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

Where it is reasonable and practical to do so, the College will collect personal information directly from the individual.

Where possible the College has attempted to standardize the collection of personal information by using specifically designed forms, e.g. a Registration Form, however, given the nature of College operations, we often receive personal information by email, letters, notes, over the telephone, in face to face meetings, through financial transactions and through surveillance activities, e.g. the use of CCTV security cameras or email monitoring.

The College may also collect personal information from other people, e.g. a reference, report from a medical professional or independent sources, e.g. a telephone directory, however, we will only do so where it is not reasonable and practicable to collect the information directly.

Sometimes the College may be provided with personal information without having sought it through our normal means of collection. This is referred to as 'unsolicited information'. Where unsolicited information is collected, the College will only hold, use and/or disclose that information if we could otherwise do so had we collected it by normal means. If that unsolicited information could not have been collected by normal means, then the information will be destroyed, permanently deleted or de-identified as appropriate.

GENERAL PRIVACY PROCEDURE

- All College records will comply with the Commonwealth Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Australian Privacy Principles. The Collection, use and storage of all information is in accord with the Australian Privacy Principles. The College has in place protection for the personal information it collects and holds including locked storage to paper records and password access rights for electronic records.
- This policy is readily available, and unless prevented by law or exception, an~~d~~ individual can access their own personal information.
- The collection, use and storage of all information is in accord with the Australian Privacy Principles
- The College may need to disclose personal and sensitive information to others for educational, welfare, health and administrative purposes. The College only uses personal information for the purposes it was provided. The College may disclose personal information to:
  - Another school
  - Government departments
  - The Catholic Education Commission
  - Medical practitioners
  - People providing services to the College including coaches and specialist visiting teachers
  - Recipients of College publications, such as newsletters and magazines
  - Anyone authorised by the individual
  - Anyone to whom we are required to disclose the information by law

  This information will only be disclosed if one or more of the following apply:
  - There is consent
  - It is reasonably expected that the College use or disclose personal information in this way
  - The College is authorised or required to do so by law
  - Disclosure will lessen or prevent a serious threat to the life, health and safety of an individual or to public safety
  - Where another permitted general situation or permitted health situation exception applies
  - Disclosure is reasonably necessary for a law enforcement related activity

  Sensitive information has a higher degree of protection and will be used and disclosed only for the purpose for which it was provided, or for a directly related secondary purpose, unless the person agrees otherwise, or the use or disclosure of the sensitive information is required by law.
- Personal information will not be disclosed overseas without gaining consent.
- The College does not store personal information in the 'cloud' which means it does not reside on a server situated outside Australia.
- College staff are required to respect the confidentiality of personal information and the privacy of individuals.
- Parents/Carers have access to their personal contact details, using their security PIN, from the College Portal and should alert the College if details need updating.
- Any other personal information held by the College may be requested by contacting the College. The discretion to reveal this is in the hands of the Principal or Deputy Principal. Access may be denied if it has an unreasonable impact on the privacy of another, where it would breach the College duty of care to students or where information has been provided in strict confidence and the release of it is not required by law.
- The College treats voicemails and other sound encodings as being subject to the Privacy Act.
- It is not permitted to record or film any person without their consent using any device.
- A form requesting permission for the disclosure of a student's name or image in the Newsletter, the College Yearbook on the Internet or the Website or for use in promotional material or in papers or other media is

distributed annually. A failure to return this form indicating your wishes will be treated as a refusal to grant permission.

Notifiable Data Breach Response Procedure

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988* (Privacy Act) established requirements for entities in responding to data breaches. The College has a data breach notification obligation when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach. See the Notifiable Data Breach Response Procedure below.

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 Deputy Principal. The Deputy Principal, with the IT Manager, 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 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, the Deputy Principal must consider if any of the affected individuals should be notified immediately where serious harm is likely.
  5. The 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**
  7. 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.
  8. 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.
  9. 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 Eligible Data Breach (EDB).

10. The response team should also consider whether any of the limited exceptions apply to the Data Breach if it is otherwise an EDB.
11. 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**
  12. 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.
  13. 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.
  14. 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.
  15. 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**
  16. 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.
  17. The Executive Assistant must enter details of the Data Breach and response taken into a Data Breach log. The IT Manager must, every year, review the Data Breach log to identify any reoccurring Data Breaches.
  18. The Deputy Principal and IT Manager 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.
  19. The Deputy Principal and IT Manager must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Data Breach Response Protocol.
  20. The Deputy Principal and IT Manager 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**
  The Response Team consists of the College:
  - Principal
  - Deputy Principal
  - Director of Business Services
  - IT Manager
  - Counsellor

Implementation

This policy is implemented through a combination of:

- Effective policies and procedures;
- Staff training in student welfare, mental health, positive psychology, positive education principles and wellbeing
- Well formulated, flexible Pastoral Care Programming;
- Effective incident notification procedures.

Discipline for Breach of Policy

Where a staff member breaches this policy Stella Maris College may take disciplinary action.

Related Documents

1. Information Communication and Technology Policy
2. Information Communication and Technology Laptop Usage Policy
3. Information Communication and Technology Social Networking Policy
4. Staff Code of Conduct Policy
5. Critical Incident Management Policy
6. Responsible Digital Citizen Protocol

Key Reference

This policy has been developed having regard to the:

- Commonwealth Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012;
- Health Records and Information Privacy Act 2002;
- Privacy Amendment (Notifiable Data Breaches) Act 2017.

VERSION 5
Policy Approved: August 2018
Date for Review: August 2021