Privacy Policy

POLICY

This Privacy Policy sets out how Mount Sinai College manages personal information and your rights in relation to your personal information, including how to complain and how we deal with complaints.

The College is bound by the Australian Privacy Principles contained in the *Commonwealth Privacy Act 1988* (Privacy Act). In relation to health records, the College is also bound by the Health Privacy Principles which are contained in the *Health Records and Information Privacy Act 2002* (NSW).

Under the Privacy Act and the Health Records Act, the Australian Privacy Principles and NSW Health Privacy Principles do not apply to certain treatment of an employee record. As a result, this Privacy Policy does not apply to the College's treatment of an employee record held by the College, where the treatment is directly related to a current or former employment relationship between the College and the employee.

The College may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the College's operations and practices and to make sure it remains appropriate to the changing College environment. The current version of this Privacy Policy is published on the College website (www.mountsinai.nsw.edu.au) .

Kinds of Personal Information we Collect

The types of information the College collects include (but is not limited to) personal information, including health and other sensitive information, about:

- students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the College, including any other general kinds of information
    - name, contact details (including next of kin), date of birth, gender, language background, previous College, and religion
    - parents' education, occupation, language spoken at home, nationality, and country of birth
    - health information (e.g., details of disability and/or allergies, dietary requirements, absence notes, immunisation details, medical reports, and names of doctors)
    - results of assignments, tests, and examinations
    - conduct and complaint records, or other behaviour notes, and College reports
    - information about referrals to government welfare agencies
    - counselling reports
    - health fund details and Medicare number
    - any Family Court orders

  - criminal records
  - volunteering information
  - photos and videos at College events
- job applicants, volunteers, and contractors, including any other general kinds of information
  - 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
  - health information (e.g., details of disability and/or allergies, and medical certificates)
  - complaint records and investigation reports.
  - leave details.
  - photos and videos at College events.
  - workplace surveillance information; and
  - work emails and private emails (when using work email address) and Internet browsing history; and
- other people who encounter the College, including name and contact details and any other information necessary for the contact with the College.

How we Collect Personal Information

Personal information you provide: The College collects personal information about an individual directly from the individual (or their Parent in the case of students). This includes by way of forms, face-to-face meetings and interviews, emails, and telephone calls.

Personal information provided by other people: In some circumstances the College may be provided with personal information about an individual from a third party, for example a report provided by a medical professional, a reference from another College or a referee for a job applicant. If a student transfers to a new College, the new College may collect personal information about the student from the student's previous College to facilitate the transfer of the student.

Personal information generated by artificial intelligence (AI) systems:

The college might also collect personal information using AI systems to generate personal information. The kinds of personal information that may be generated by AI systems include those set out above under the heading '*Kinds of Personal Information we Collect*'

Personal information from other sources: We may also collect personal information through surveillance activities (such as 24/7 CCTV security cameras) and student and staff email monitoring.

Purposes for Which we Collect, Use, and Disclose Personal Information.

The purposes for which the College collects, uses and discloses personal information depend on our relationship with you and include the following:

Students and Parents:

- providing schooling and College activities
- satisfying the needs of Parents, the needs of students and the needs of the College throughout the whole period a student is enrolled at the College
- making required reports to government authorities
- keeping Parents informed about matters related to their child's schooling, through correspondence, apps, newsletters, and other publications
- day-to-day administration of the College
- looking after students' educational, social and health wellbeing
- seeking donations for the College (see the 'Fundraising' section of this Privacy Policy)
- to satisfy the College's legal obligations and allow the College to discharge its duty of care.

Volunteers:

- to contact you about, and administer, the volunteer position
- for insurance purposes; and
- satisfying the College's legal obligations, for example, in relation to child protection legislation.

Job applicants and contractors:

- assessing and (if successful) engaging the applicant or contractor
- administering the individual's employment or contract
- seeking donations for the College (see the '*Fundraising and Marketing*' section of this Privacy Policy)
- for insurance purposes
- satisfying the College's legal obligations, for example, in relation to child protection legislation.

Automated Decision Making

The college may use personal information in the operation of computer programs to make or assist us in making certain decisions (automated decisions). The personal information we use for this purpose is listed above under '*Purposes for Which we Collect, Use and Disclose Personal Information*'. The decisions we make using this personal information in the operation of computer programs may include:

- those that may be reasonably expected to significantly affect the rights or interested of an individual, and where that information is used in the operation of a computer system (AI) to make the decision or as a substantial input to the making of the decision e.g., whether a student has the prerequisite experience to participate in a particular course or college activity.
- other decisions as notified by the college from time to time.

Who we Disclose Personal Information to

The College may disclose personal information, including sensitive information, for educational, care and administrative purposes, and to seek support and advice. This may include to:

- other Colleges and teachers at those Colleges, including a new College to which a student transfers to facilitate the transfer of the student
- government departments (including for policy and funding purposes)
- medical practitioners
- people providing educational, support and health services to the College, including specialist visiting teachers, sports coaches, volunteers, and counsellors
- organisations that assist us with fundraising (see the '*Fundraising and Marketing*' section of this Privacy Policy)
- providers of specialist advisory services and assistance to the College, including in Human Resources, child protection, students with additional needs and for the purpose of administering Online Apps for Education and ensuring its proper use (see further the section below '*Sending and Storing Information Overseas'*)
- 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) and NESA
- 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 College
- the provider of our information management and storage system and other information technology services
- recipients of College publications, such as newsletters and magazines
- students' parents or guardians
- anyone authorised by the College to disclose information to; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.
- The College may disclose personal information to a third-party provider as part of the College's use of AI systems.

How we Store Personal Information

We store your personal information in hard copy and electronically. We currently use an Information Management and Storage System called TASS. Personal information may at times be accessible by the third-party service providers for the purpose of providing services to the College in connection with the systems.

The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information. See further the section below '*Sending and Storing Information Overseas*.'

Sending and Storing Information Overseas

The College may disclose personal information about an individual to overseas recipients in certain circumstances, for instance, to facilitate a College exchange.

The College may use online or 'cloud' service providers to store personal information and to provide services to the College 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 and provide technical support. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's server which may be situated outside Australia.

Personal information may be used for training the College's AI systems or for other purposes associated with AI systems not already listed here. The personal information used may include that of volunteers, job applicants and/or contractors.

An example of such a cloud service providers are Google or Microsoft 365. Google provides Apps for education (GAFE) including Gmail, and stores and processes limited personal information for this purpose. School personnel and the AIS and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g., instant messaging) documents and associated administrative data for the purposes of administering GAFE and ensuring its proper use. Microsoft 365 is used in a similar manner.

The college may use AI systems that are provided by third parties. These third parties may store or have access to personal information input into, and/or generated by these AI systems. These third parties may be located outside of Australia. The College will keep records of which countries this may entail.

Fundraising and Marketing

The College treats seeking donations for the future growth and development of the College as an important part of ensuring that the College continues to provide a quality learning environment in which both students and staff thrive. Your personal information may be used to make an appeal to you. It may also be disclosed to organisations that assist in the College's fundraising activities, for example, the College's Foundation and, on occasions, external fundraising organisations.

If you do not want to receive fundraising communications from us, please contact our the Director of Finance and Operations via the school email address reception@mountsinai.nsw.edu.au .

Security of Personal Information

The College has in place steps to protect the personal information the College 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.

These steps include:

- Restricting access to information on the College databases on a need-to-know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where personal and health information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need-to-know basis.
- Implementing physical security measures around the College buildings and grounds to prevent break-ins. This includes the use of security guards at the front entrance and patrolling the perimeter of the campus. The College has installed sophisticated, 24/7 CCTV along the perimeter and within the College campus. Videos are viewed everyday by security and designated staff members and copies of the videos are stored daily on the College network and the Cloud. Mount Sinai may view video from its CCTV cameras located around the College campus to investigate incidents of misbehaviour or accidents and to identify the individuals involved, in line with the *Workplace Surveillance Act 2005*.
- Implementing ICT security systems, policies, and procedures, designed to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, confidentiality, and document security policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure

- as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Access and Correction of Personal Information

Under the Commonwealth Privacy Act and the Health Records Act, an individual has the right to seek access to, and/or correction of, any personal information which the College holds about them. Students generally will be able to access and update their personal information through their Parents.

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

To make a request to access, update or correct any personal information the College holds about you or your child, please contact the College Principal, their Personal Assistant or the College Receptionist, by email, or telephone at (02) 9349 4877. The College may require you to verify your identity and specify what information you require. Or are correcting. The College may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). If the information sought is extensive, the College will advise the cost in advance.

If we decide to refuse your request, we will provide you with written notice explaining the reasons for refusal (unless, considering the grounds for refusing, it would be unreasonable to provide reasons) and how to complain.

Consent and Rights of Access to the Personal Information of Students

The College respects every Parent's right to make decisions concerning their child's education.

Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. The College 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 College about them or their child by contacting the College Principal or their Personal Assistant by telephone or in writing (details in the section above '*Access and Correction of Personal Information*').

However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where the College believes the student has capacity to consent and the College is not permitted to disclose the information to the Parent without the student's consent, 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 College's duty of care to the student.

The College may, at its discretion, on the request of a student grant that student access to information held by the College about them or allow a student to give or

withhold consent to the use of their personal information, independently of their Parents. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Enquiries and Complaints

If you would like further information about the way the College manages the personal information it holds or wish to make a complaint about a perceived breach of the Australian Privacy Principles, or the Health Privacy Principles please contact the College Principal by email, post, or telephone at (02) 9349 4877. The College 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.

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC) via the OAIC website, www.oaic.gov.au.

The Director of Finance and Operations may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the Colleges' operations and practices and to make sure it remains appropriate to the changing College environment. The current version of this Privacy Policy is published on our website (www.mountsinai.nsw.edu.au).

Policy & Procedure	**Mount Sinai Privacy Policy**
Owner	**Principal**
Date	8-10-24
Changes	22-5-25
Date for Review	05-06-27