PRIVACY POLICY

HALE SCHOOL

1. Purpose

The purpose of Hale School's (Hale/the School) Privacy Policy (the Policy) is to provide direction on the collection, use, management, and disclosure of personal information provided to, or collected by it, while discharging its mission. This document must be read in conjunction with the school's Archival Records Management Policy and Archives Policy

Hale School is bound by and complies strictly with the Australian Privacy Principles (APP) contained in the Commonwealth Privacy Act (1988) and Schedule 2 of the amended Privacy Act (1988) as well as the Privacy and Other Legislation Amendment Act (2024). In relation to health records, the school is also bound by the Health Services (Conciliation and Review) Act 1995 and the Freedom of Information Act 1992.

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

The provisions of this Policy apply to the entire Hale School Community in collecting, holding, accessing, and using personal and sensitive information from and about, but not limited to:

- Current and prospective students;
- Current and prospective parents/guardians;
- Current and prospective staff;
- Old Haleians;
- Current and prospective donors;
- Current and prospective suppliers and contractors;
- Volunteers; and
- Users of the School's facilities, services, events or activities.

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 relevant to the changing School environment. As an example, it is anticipated the School will in late 2026 align this Privacy Policy with the Children's Online Privacy Code being developed by the Office of the Australian Information Commissioner to introduce new privacy protections for children engaging with digital services.

The current version of this Privacy Policy is published on our website.

2. Definitions

Doxxing

Doxxing is the use of a carriage service to make available, publish or distribute personal data (i.e. information about an individual that enables them to be identified, contacted or located), where the person engages in the conduct in a way that reasonable persons would regard as being menacing or harassing.

Eligible Data Breach

An eligible data breach under the Privacy Act 1988 is either:

- unauthorised access or disclosure of personal information where a reasonable person would conclude that the disclosure or access is likely to result in serious harm to those individuals affected, or
- where information is lost in circumstances where unauthorised access or disclosure is likely to occur and assuming that if unauthorised access or disclosure were to occur, a reasonable person would conclude that the disclosure or access is likely to result in serious harm to the affected individuals.

Health Information

Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected while providing a health service.

Personal Information

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source.

Sensitive Information

Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a

trade union, sexual orientation or practices, or criminal record. It also includes health information and biometric information.

3. Policy Statement/Principles

3.1 Personal Information Collected, methods of collection and storage

The types of information the school collects and holds includes (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 school,
- job applicants, staff members, volunteers, and contractors; and
- other people who may come into contact with the School.

The school will collect Personal Information where that information is reasonably necessary for the performance of one or more functions and/or activities of the school.

The school will collect personal information by lawful, fair and transparent means and wherever possible, directly from the individual.

The School will generally collect personal information held about an individual by way of forms completed (in hard copy or online) by a parent or student, in face-to-face meetings, interviews, emails and telephone calls.

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. This personal information will be treated in the same manner as if it were collected by the school.

The School takes, stores and uses images and videos of students in the course of providing a range of educational services and co-curricular activities.

If the School receives personal information about a third party from an individual, that individual must ensure that:

- the information is correct and has been collected and disclosed in accordance with the Act;
- the individual is entitled to disclose that information to the school; and
- without taking any further steps, the school may collect, use and disclose that information in accordance with this policy.

Personal information is stored in hard copy onsite and in electronic format in relational databases and as individual files on both cloud and onsite file systems. Methods of information storage include magnetic storage (like hard drives and tapes), solid-state storage (such as SSDs and flash drives), and optical storage (CDs, DVDs) for physical media, alongside digital methods like cloud storage, server attached storage arrays and network-attached storage (NAS).

3.2 Use of personal information

The School will use personal information it collects only 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 the provider, or to which the provider has consented.

Hale School's primary purpose for collection of personal information relating to students and parents is to enable it to provide schooling and educational services to the student and includes:

- Pre-enrolment matters;
- Keeping parents informed about matters related to their child's schooling, through correspondence, newsletters, magazines and other publications;
- Day-to-day administration;
- Looking after students' educational, social and medical wellbeing;
- Drawing upon the expertise of particular members of the School community to assist with operations and functions;
- Seeking donations for the School;
- Promotion and marketing of 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 requested personal information about a student or parent is not provided, the School may be unable to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

The school's primary purpose for collection of personal information of job applicants, staff members, contractors and volunteers is to assess suitability for engagement, for administering contracts, insurance purposes and to satisfy legal obligations, for example, in relation to child protection.

Personal information held by the School may be disclosed to an organisation that assists in the School's marketing and fundraising endeavours, such as the Hale School Parents' and Friends' Association, the Hale School Foundation (Inc), or the Old Haleians' Association.

3.3 Disclosure of personal information

The School may disclose personal information, including sensitive information, held about an individual to:

- Another school;
- Agencies and Government departments to whom we are required to disclose personal information for education, funding and research purposes;
- Medical practitioners;
- People providing services to the School, including specialist visiting teachers, counsellors and sports coaches;
- 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);
- People providing administrative and financial services to the School e.g. the School's external auditors and Legal Counsel;
- Recipients of School publications, like newsletters and magazines;
- Fundraisers seeking donations for the School
- Parents to keep them informed about matters related to their child's schooling, through correspondence, newsletters, magazines and "apps"; and
- Anyone to whom the provider authorises the School to disclose information.
- Anyone to whom the school is required to disclose the information by law, including child protection laws.

The School will take care when taking using and sharing photographs and video footage which includes individuals. Consideration will be given as to whether informed consent is required particularly where a student or parent was not aware that the photo or footage could be used or published for a particular purpose, or published in a particular place such as the website, social media or the School's newsletter, yearbook and other such publications in these locations.

Subject to obtaining completed Annual General Consent Forms or a Standard Collection Notice, the School will share photographs and footage of students with the School Community for the purpose of reporting on school activities and events. This includes sharing via locations that are only accessible by members of the School community.

The School will use a specific consent form for situations which may not be covered by the general consent. This includes specific marketing campaigns, regardless of whether general consent for marketing has been obtained.

The School will purchase and implement a media management tool, in 2026. ISO27001 certified, it is expected to streamline and improve daily administration and handling of photos, videos, and associated media, It will enable the school to seamlessly link consent data with media.

Where possible photographs and images of students and staff will be de-identified before they are printed or published in School publications or posted to School social media sites.

The School ensures that its students and staff are aware that the Privacy and Other Legislation Amendment Act 2024 (Cth) made 'doxxing' a criminal offence and engagement in this practice will result in disciplinary action.

The School may disclose personal information about an individual to overseas recipients, for instance, to Universities in the UK and USA to facilitate scholarships for students, a school exchange or when storing personal information with "cloud" service providers, after:

- Obtaining consent from the provider (in some cases this consent will be implied), or
- Otherwise complying with the Australian Privacy Principles or other applicable privacy legislation

Where the overseas recipient is not in a country bound by Privacy Legislation that is consistent and comparable with Australian Privacy laws, the School will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the Australian Privacy Principles (APP). This means compliance with the APP in relation to the collection, use, disclosure,

storage, destruction or de-identification of personal information, the complaint handling process for privacy complaints and implement a data breach response plan including notifying the School where there are reasonable grounds to suspect a data breach and outline appropriate remedial action.

3.4 Treatment of Sensitive Information

Sensitive information will only be used and disclosed for the purpose for which it was provided, or directly related secondary purpose, unless the provider's express agreement has been obtained to do otherwise, or the use or disclosure of the sensitive information is allowed by law.

3.4.1 Health Information

Hale School collects health information about its students, staff and on occasions, parents:

- With the consent of the student or parent;
- Where it is required to enable the school to exercise its duty of care or is otherwise required or authorised by law;
- Where the School itself records incidents at school;
- Where a student suffers an injury or illness, a school nurse, school psychologist assesses, makes a diagnosis of illness or disability, treats a student and creates and maintains records of the student's progress;
- Where it is necessary to lessen or prevent a serious threat to the life, health, or safety of an individual and it is impracticable to obtain consent.

Health information will only be used or disclosed:

- For the purposes for which it was collected or a directly related secondary purpose;
- To exercise the school's duty of care or as otherwise required or authorised by law; or
- To lessen or prevent a serious threat to the life, health, or safety of an individual and where it is impractical to obtain consent.

Health information is securely stored and only staff who have a need to know the information are provided access to it. Health information of a student is not disclosed to third parties, such as another parent or an organisation or school which may have temporary care of the student unless the School considers it is necessary to disclose it to ensure the health or safety of the student.

The school will seek expert advice in any instance where it becomes aware of health information about a student which the student does not wish to be disclosed to a parent or both parents.

3.5 Management and security of personal information

A statutory tort for serious invasion of privacy is in effect under Schedule 2 of the Amended Privacy Act 1988 (Cth). The School recognises it may be sued for privacy breaches including:

- Misuse of personal information e.g. mishandling student records or health data
- Intrusion upon seclusion e.g. unauthorised surveillance or access to private spaces

These claims will need to show the breach was serious, intentional, or reckless and violated a reasonable expectation of privacy.

The school will take reasonable steps to:

- Review third party providers and strengthen data security and breach response procedures
- Regularly assess its requirements for capturing and using photographs, videos and any digital images of students and staff and avoid uploading identifiable student data and images to unsecured platforms
- Align with the *National Model Code for Taking Images or Videos of Children while providing Early Childhood Education and Care*. In relation to students over the age of 5 years, in accordance with the School's ICT Policy, wherever possible and practical staff are to refrain from using their own electronic devices (e.g. phones or cameras) to take photographs of students at Hale School. When photographs are taken on a personal device, the image is to be uploaded to an appropriate Hale site as soon as possible and images on a file, card or device are to be erased. The deletion must include any cloud backups the personal phone or camera has made
- Destroy or de-identify personal information which is no longer needed for the school's business or required to be retained under law, regulation or any code applicable to the School;
- Ensure that the personal information it collects, uses or discloses (having regard to the purpose of the use of disclosure) is accurate, up to date and complete;
- Ensure that the systems, tools, and methods of capturing, transmitting and holding information in all formats are protected from misuse, interference, loss and from unauthorised access, modification or disclosure. However, the School

cannot be held responsible for the theft of data by a third party, or the loss of data through technical or technological malfunction, tampering by a third party, or any event that is beyond the reasonable control of the School.

3.6 Use of Artificial Intelligence (AI) systems

- The School has governance processes in place and has clearly defined the permitted use of certain AI systems and the personal information that may be used in relation to those systems. Conducts AI training for staff and students in the systems approved for use
- Provides directions on how AI can or cannot be used
- Does not permit the input of personal information in publicly available systems
- Has established procedures for explaining AI-related decisions and outputs to affected individuals
- Ensures AI systems have human oversight and that reasonable steps are taken to verify any personal information generated by AI systems.
- Surveys staff in relation to their use of AI systems.

3.7 Access and correction of personal information

Under the Privacy Act, an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any inaccuracy. There are some exceptions to this right set out in the Act. Students will generally have access to their personal information through their parents, but older students may seek access themselves.

To make a request to access any information the school holds about a student or his parent(s), it will be necessary to submit a request in writing to the Headmaster.

The school may charge a fee to recover any costs incurred because of verifying the identity of an applicant, clarifying the specific request in the application, locating, retrieving, reviewing and copying any material requested. If the information sought is extensive the school will advise the likely cost of this service in advance.

Where a person believes their personal information held by the School is not accurate, they may seek to update their personal information by contacting the Director of Finance & Governance (who represents the School as its Privacy Officer) during business hours.

3.8 Consent rights of access to personal information of students

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's parent(s). 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.

In accordance with section 3.7 above, parents may seek access to personal information held by the school about them or their child by contacting the Headmaster. There will, however, 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 breach of the School's duty of care to the student.

The School may, at its discretion, upon 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 student and/or the student's personal circumstances so warrants.

3.9 Enquiries and complaints

Enquiries from a student or his parent about the way in which the school manages the personal information it holds, or complaints that the school has breached the Australian Privacy Principles, may be addressed to the Headmaster or the Director of Finance and Governance who is the School's Privacy Officer. The school will investigate all complaints and will notify the complainant of the outcome of the investigation and any related decision as soon as practicable.

3.10 Breaches of Policy

Failure to comply with this policy may be considered a breach of the Code of Ethics and Code of Conduct and may result in disciplinary action.

3.11 Eligible Data Breaches

The school will notify the Office of the Australian Information Commissioner and an individual affected by a breach of this Policy, where there is a breach, and that breach is categorised as an eligible data breach. Notification to the OAIC will be within 72 hours.

4. Related Legislation

- Commonwealth Privacy Act (1988)
- Privacy and Other Legislation Amendment Act 2024
- Amended Privacy Act (1988) Schedule 2

PRIVACY POLICY

HALE SCHOOL

- Australian Privacy Principles within the Commonwealth Privacy Act
- Health Services (Conciliation and Review) Act 1995
- Freedom of Information Act 1992

Related Policies

- Archives Policy
- Archival Records Management Policy
- Child Protection and Mandatory Reporting Policy
- Child Safety Policy
- Dispute and Complaints Policy (students/parents/community)
- Information and Communication Technology Policy

Date originally approved:	***Approving authority:***
October 2022	Director of Staff Development and Human Resources
Date this version approved:	***Date policy to be reviewed:***
December 2025	December 2025
Policy Custodian: (Contact for queries)	***Policy Category:***
Director of Finance and Governance	Facilities and General Management

Policy Version
4
Changes Made
Inclusion of provisions of a statutory tort for serious invasion of privacy and the School's response and alignment with the National Quality Framework of digital safety measures in early childhood education and care. Addition of section on doxxing, use of AI systems, protocols and requirements for taking, using and sharing photographs and video footage of individuals.