Hunter Valley Grammar School

Policy

Privacy Policy

Introduction

This Privacy Policy sets out how Hunter Valley Grammar School manages personal information and your rights in relation to your personal information, including how to complain and how we deal with complaints.

The School is bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act 1988 ('Privacy Act'). In relation to health records, the School is also bound by the New South Wales Health Privacy Principles which are contained in the Health Records and Information Privacy Act 2002 ('Health Records Act').

Under the Privacy Act and the Health Records Act, the Australian Privacy Principles and Health 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 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. The current version of this Privacy Policy is published on PolicyConnect and the School website.

Kinds of personal information we collect

The type of information the School collects 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 pupil's enrolment at the School, including:
  - 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 name of doctor;
  - Conduct and complaint records, other behaviour notes, and school reports;
  - Health fund details and Medicare number;
  - Any court order;

  - 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, and
- other people who come into contact with the School.

How we collect personal Information

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

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, a reference from another school or a referee for a job applicant. If a student transfer to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.

Personal information from other sources: We may also collect personal information through surveillance activities (such as CCTV security cameras) and email filtering.

Purposes for which we collect, use and disclose personal information

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

Students and Parents:

- providing schooling and school activities;
- satisfying the needs of Parents, the needs of students and the needs of the School
- throughout the whole period a student is enrolled at the School;

- making required reports to government authorities;
- keeping Parents informed about matters related to their child's schooling, through
- correspondence, apps, newsletters and magazines;
- day-to-day administration of the School;
- looking after students' educational, social and health wellbeing;
- seeking donations for the School (see the 'Fundraising' section of this Privacy Policy); and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

Volunteers

- to contact you about, and administer, the volunteer position;
- for insurance purposes; and
- satisfying the School'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 School (see the 'Fundraising' section of this Privacy Policy);
- for insurance purposes; and
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Who we disclose personal information to

The School may disclose personal information, including sensitive information for educational, administrative and support purposes. This may include to:

- other schools and teachers at those schools, including a new school 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 School, including specialist visiting teachers, coaches, volunteers and counsellors;
- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection, student with additional needs and for the purpose of administering ICT systems that support these services (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 Administrative

Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);

- agencies and organisation to whom we are required to disclose personal information for education, funding and research purposes
- people providing administrative and financial services to the School;
- the provider of our information management systems including but not limited to student information, learning management and compliance systems.
- recipients of School publications, such as newsletters and magazines;
- students' 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.

How we store personal information

We store your personal information in hard copy and electronically. We use information management and storage systems provided by third party service providers. Personal information is stored with and accessible by the third party service providers for the purpose or providing service to the School in connection with those services.

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. See further section below 'Sending and storing information overseas'.

Sending and storing information overseas

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

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 and provide technical support.

The School has systems and processes in place for the review and approval of all software and ICT systems used in the School. This includes a review of the compliance of all systems with the Australian Privacy Principles, an assessment of the compliance of the system with the General Data Protection Regulation (GDPR - the personal data protection requirement adopted by Europe), and determination of the purpose, accessibility and sovereignty of all data used and stored by the system. The Director of ICT has the final approval for all software use in the School and ensure that all systems meet these requirements.

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.

An example of such a cloud service provider is Microsoft 365. Microsoft 365 is a suite of productivity and collaboration products including Outlook, which stores and processes limited personal information as part of using these products. School personnel 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 Microsoft 365 and ensuring its proper use.

Fundraising and Marketing

The School treats 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 students and staff thrive. Your personal information may be used to make an appeal to you. If you do not want to receive fundraising communications from us, please our Communication Teams via email at communityrelation@hvgs.nsw.edu.au.

Security of personal information

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.

These steps include:

- Restricting access to information on the School 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 School buildings and grounds to prevent break-ins.
- Implementing ICT technical controls, policies and procedures, designed to protect personal information storage on our computer networks.
- Implementing human recourses 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.

- Ensuring that data retention and destruction protocols are in place and followed as per our Record Management Policy and other related guidelines that support the requirements of Australian Privacy Principle 11.2

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 School holds about them and to advise the School of any perceived inaccuracy. Pupils 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.

Parents may seek access to personal information held by the School about them or their child by contacting the School Principal in writing. However, there will 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 require parents to verify their identity and specify what information they require. The School may charge a fee to cover the cost of verifying an 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 the School cannot provide access to the information requested, the School will provide written notice explaining the reasons for refusal.

The School respects every Parent's right to make decisions regarding 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.

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 pupil reaches 18 years of age 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 the School has breached the Australian Privacy Principles please contact the School Principal via email

principal@hvgs.nsw.edu.au, or telephone at (02) 49342444. The School will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as it is practicable after it has been made.

Resources

The School will provide the appropriate resources and structure to facilitate the implementation of this policy. The Principal, supported by the Compliance Manager, is responsible for the implementation of this Policy.

Related Documents

This policy should be read in conjunction with the following related documents:

- Mandatory notification of Eligible Data Breach – Summary
- Data Breach Response Plan
- Data Breach Risk Assessment Factors
- Staff Code of Conduct
- Child Safe Policy

Child Safe Standards

This Policy supports the implementation of the following Child Safe Standards

Contacts

Governance Officer: Compliance Manager

Accountable Officer: Principal

Responsibilities

Position	Responsibility
Board	The Board is the Approver for this Policy
Compliance Manager	The Compliance Manager is responsible for ensuring implementation and communication of this policy
Principal	The Principal is responsible for ensuring that this Policy is adopted.

Definitions

Term	Meaning
Privacy Principles	The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers. There are 13 Australian Privacy Principles.
CCTV	Closed Circuit Television

Evaluation

The Board is responsible for evaluating compliance with the policy. Evaluation will be facilitated by means of:

- Compliance Report to the Risk and Compliance Committee;
- Principal's Report to every Board Meeting;
- Minutes from Board Committee Meetings;

Document information and review

This policy document will be reviewed at least every three years.

Review Due: June 2026

Policy Code:	**POL-PRV-001**
Approved By:	Board
Approval Date:	16 August 2023
Effective From:	1 September 2023

Approval History

Version	Date	Description
1	June 2007	New policy document endorsed by the board
2	May 2011	Policy document reviewed and amended
3	March 2014	Policy document reviewed and amended
4	May 2017	Policy document reviewed and amended
5	February 2019	Policy document reviewed and amended
6	August 2023	Policy document reviewed and amended