IVANHOE
GRAMMAR SCHOOL
courageous and kind

Privacy Policy

1. Statement of Context and Purpose

Pursuant to Commonwealth privacy laws, Ivanhoe Grammar School (**the School**) is required to have a privacy policy which is available to all people associated with the School

Privacy laws regulate how the School can collect, use, hold and disclose personal information. The school is bound by the Australian Privacy Principles (**APPs**) contained in the *Privacy Act 1988* (Cth) (**Privacy Act**). The information the School collects enables it to provide educational services and discharge its duty of care.

2. Scope

This policy describes protection of personal (including sensitive) information obtained, held, used and disclosed by the School. It applies to all employees (where applicable), students, volunteers, contractors, visitors and other people who are associated with or come into contact with the School.

3. Policy

3.1 Dealing with the School Anonymously and Pseudonymously

In accordance with the APPs, individuals have the option of not identifying themselves at all or of using a pseudonym when dealing with the School in relation to a particular matter.

However, this option will not apply if:

- the School is required or authorised by or under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves concerning that matter; or
- it is impracticable for the School to deal with individuals who have not identified themselves or who have used a pseudonym on a particular matter.

3.2 Types of Personal Information Collected

The School collects personal information, including sensitive information, about:

- students;
- parents or designated carers;
- employees (where applicable) and prospective employees;
- contractors and prospective contractors;
- volunteers;
- visitors;
- alumni; and
- any other person who comes into contact with the School.

The types of personal information that the School collects includes information such as name, age, contact details, academic records and history, tax file numbers, work history, images (including photos, surveillance and CCTV footage) and sensitive information including information about a student's health, religion or racial or ethnic origin.

3.3 How will Sensitive Information be treated?

Sensitive Information about an individual will not be collected unless one of the following applies:

- the individual consents to the collection of Sensitive Information from the individual and the information is reasonably necessary for one or more of the School's functions or activities; or
- the collection of Sensitive Information is required or authorised by or under an Australian law or a court/tribunal order.

3.4 Collection of personal information

A person who collects Personal Information (including Sensitive Information) on behalf of the School must comply with this policy and the requirements of the Privacy Act. This includes taking reasonable steps to make sure the individual is aware of:

- the School's identity and contact details;
- the fact and circumstances of collection;
- whether the collection is required or authorised by law;
- the purposes of collection;
- the consequences if Personal Information is not collected;
- the School's usual disclosures of Personal Information of the kind collected by the Company;
- information about this Privacy Policy; and
- whether the School is likely to disclose Personal Information to overseas recipients, and if practicable, the countries where they are located.

3.5 How Personal Information will be collected and stored

The School will make individuals aware of the purpose for which information is collection by notifying them about all the relevant matters of that collection.

Information about individuals may be collected in a number of ways including:

- directly from students, parents and guardians by telephone, in written and online applications and forms or in person;
- collection statements;
- from other parties (such as past schools or employers, referees, social media sites medical practitioners or other schools);
- CCTV cameras or other security protection measures;
- from the Company's website using various technologies, including cookies; and
- from publicly available sources.

The School may store information either electronically or physically in the following ways:

- on electronic files or databases with password protection; or
- in a secure location, including lockable cabinets with access only to authorised personnel.

3.6 Use and Disclosure of Information

The School will use or disclose 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 reasonably expected, or to which you have consented or otherwise as permitted by legislation.

The School collects and uses personal information for the primary purpose of providing schooling and educational services for its students, including to:

- implement the School's Strategic Intent;
- satisfy legal obligations including with respect to legislation, including child protection legislation, relevant to the School;
- administer accounting, administrative and other business functions of the School;
- manage relationships, safety, social emotional, psychological and medical issues and wellbeing of students and parents;
- facilitate the exchange of information between schools in the context of student transitions;
- support alumni and community-based organisations and charities;
- recruit, onboard and develop current and future employees, contractors and volunteers; and
- promote the School through marketing and school publications.

In relation to surveillance and CCTV footage collected about any person that comes into contact with the School, the School will use or disclose that information in accordance with applicable legislation.

If a person does not wish personal information (including images) relating to them to be used for the above purposes they should issue a request to the School's Privacy Officer via the email address privacyofficer@ivanhoe.com.au.

Marketing

Parents, staff and other relevant individuals may from time-to-time receive fundraising information. School publications, such as newsletters and magazines, may include personal information (other than sensitive information).

If you do not want to receive marketing materials from the School, you may contact the Communications and Marketing Manager via email address Kristina.Garla@ivanhoe.com.au to have your name removed from the mailing list.

3.7 To whom might the School disclose personal information to?

The School may disclose personal information (including CCTV footage) to:

- provide schooling for its students
- other schools;
- government departments or authorities;
- medical or treating practitioners;
- people providing services to the School;
- recipients of the School's publications;
- parents; and
- anyone else that the School may disclose information to in accordance with the performance of its function.

Personal information may be disclosed to organisations that assist in the School's fundraising. Parents, employees, contractors and other members of the wider School community may from time to time receive fundraising information.

Overseas Recipients

Disclosure to overseas recipients may occur when dealing with overseas service providers. For example storing of information with 'cloud' suppliers or supplying information to facilitate overseas student exchange or trip providers. Countries that the School is likely to send personal information to include USA, China, India, Vietnam and Cambodia.

The School will not send information about an individual outside Australia without otherwise complying with the APPs or other privacy legislation including obtaining consent from the relevant individual.

3.8 Information Quality

The School will take reasonable steps to ensure that the personal information that is collected, used and disclosed is accurate and up-to-date. For example, the School will update its records as soon as practicable when an individual provides any new information or information that has changed. Individuals may seek access to personal information held about themselves as advised by the 'Access to Information' section of this policy. Inaccuracies in information supplied should be advised to the Privacy Officer via the email address privacyofficer@ivanhoe.com.au.

3.9 Integrity of Information

The School will take such steps that are reasonable to protect personal information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

This includes taking appropriate security measures such as:

- using locked storage, password protection, secure restricted access databases etc to protect electronic materials and material stored and generated in hard copy; and
- 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 APPs or a similar privacy regime.

The School will take reasonable steps to ensure that information is destroyed or de-identified when it is no longer required by law or for foreseeable primary or secondary purposes. Unsolicited personal information will be destroyed.

3.10 Data Breaches

Any data breaches are required to be notified to the School's Privacy Officer who will:

- carry out an investigation as soon as possible which must be completed within 30 days;
- act quickly to reduce the level of any harm;
- review internal security measures and implement corrective action if required; AND
- record any actions taken.

If the investigation reveals that the data breach could result in serious harm it must be reported to the affected individuals and the Office of the Australian Information Commissioner (**OAIC**). If affected

individuals are unable to be notified the School will publish a statement on the School's website and take reasonable steps to publicise the contents of this statement.

3.11 Access to Information

Parents and students may request access to personal information held by the School about that individual. An individual has a right to obtain access to his or her personal information under the Privacy Act and other legislation with some exceptions.

Parents may request access to personal information held by the School collected about their child. It is the responsibility of the School to ensure that they do not disclose information which would have an unreasonable impact on the privacy of others, where access may result in a breach of the School's duty of care to the student and legal obligations.

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 student involved had reached 18 years of age, but the School could do so in other circumstances when the maturity of the student and/or the student's personal circumstances so warranted.

Upon request, the School will provide an individual with access to their personal information, but may charge an access fee to cover the cost of retrieving and supplying the information. Requests should be made to the Privacy Officer via the email privacyofficer@ivanhoe.com.au. If the request is in relation to a students' information the request could be copied to the Head of House or Head of Year for Secondary Students and to the Classroom Teacher or Year Level Coordinator for Primary Students in order to facilitate retrieval of the information.

3.12 CCTV

The School is committed to providing and maintaining a safe environment for staff, students and visitors and fulfilling its statutory obligations under the *Surveillance Devices Act 1999* (Vic) and other relevant legislation regarding the use of surveillance devices, such as closed-circuit television (**CCTV**).

Locations

The School currently has surveillance devices in the form of CCTV cameras installed internally, externally and at various locations surrounding the Campuses including some school owned vehicles.

All surveillance devices are clearly visible, and notices are in various places informing people of their use. No form of surveillance device is installed in areas such as toilets, change rooms or any other location where individuals may reasonably expect to have a degree of privacy.

Collection, use and disclosure

The School reserves the right to access collected CCTV footage, and to use that footage as evidence where something has occurred that warrants investigation. This may occur in a range of circumstances, including but not limited to:

- injury to a staff member, student and/or visitor;
- assault of a staff member, student and/or visitor;
- complaint regarding a staff member, student and/or visitor;

- theft of property;
- damage to property;
- unlawful activity; and
- any other undesirable behaviour.

The School will not generally publish or disclose the footage obtained through the use of surveillance devices without the consent of the individuals in the recording. However, the School may be required by law to provide surveillance footage and/or audio to authorities in the event of an external investigation, or in the course of legal proceedings.

Should an individual request access to footage, that request will be dealt with in accordance with the requirements of the Privacy Act and this Privacy Policy.

Security

Any surveillance device data held by the School will be kept secure at all times. Information collected via CCTV footage will be stored and maintained electronically on a standalone server at the School. The recordings are only accessible by secure login.

Where data is required to be released to authorities, it is reasonably expected that this data will be kept secure and dealt with in accordance with relevant legislation. In such circumstances, please note that the School has limited control over the data.

Ownership

Any video surveillance data obtained shall remain the legal property of the School.

3.13 General Data Protection Regulation

The General Data Protection Regulation (**GDPR**) refers to a set of data protection requirements which aim to create clear and uniform data protection laws that apply to European Union residents. If the GDPR applies to the School, the School will the data handling regime in respect of any personal data of data subjects (residents) in the European Union that the School obtains.

The meaning of personal data under the GDPR is similar to Personal Information, however it is broader as it includes any information relating to an identified or identifiable natural person.

The School is committed to taking appropriate steps to ensure that personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for legitimate purposes;
- accurate and up to date;
- kept for no longer than is necessary for the purposes for which it was collected; and
- secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

European residents have the right to access personal data the School holds about them and to request that personal data be corrected, updated, deleted or transferred to another organisation. European residents are also able to request that the processing of their personal data be restricted or object to their personal data being processed.

To make any of these requests, please contact the School's Privacy Officer.

If there is an objection to the processing of personal data, or if consent to processing is provided but later withdrawn, the School will respect that choice in accordance with its legal obligations. However, please be aware that:

- such objection or withdrawal of consent could mean that the School is unable to provide services, and could unduly prevent the School from legitimately providing services to others; and
- even after consent is withdrawn, the School may be able to continue to keep and process personal data to the extent required or otherwise permitted by law, in particular:
    - to pursue the School's legitimate interests and which does not materially impact on an individual's rights, freedoms or interests; and
    - in exercising and defending the School's legal rights and meeting its legal and regulatory obligations.

3.14 Consent

The Privacy Act protects an individual's personal information regardless of their age. The Privacy Act does not specify an age after which an individual can make their own privacy decision. For their consent to be valid, an individual must have capacity to consent.

The School will treat consent given by parents as consent given on behalf of the student, and notice given to parents will act as notice given to the student.

3.15 Enquiries and Complaints

Any person may request further information about the way the School manages the personal information it holds by submitting a request to the Privacy Officer via the email address privacyofficer@ivanhoe.com.au.

A person who wishes to make a complaint about the School's compliance with the APPs, can submit the complaint to the Privacy Officer via the email address privacyofficer@ivanhoe.com.au.

The School will investigate any complaint and will notify the person who made the complaint of the School's decision as soon as practicable after it has been made.

---

4. Roles and Responsibilities

The School's Privacy officers are responsible to:

- be familiar with the Privacy Act and regulations;
- ensure a privacy impact assessment is carried out whenever the school changes the way we collect, collate or display personal data;
- ensure the register of personal information collected and displayed by the School is kept up to date; and
- investigate all reported privacy breaches and report any privacy breaches that have been deemed to have potential to cause serious harm to the OAIC.

Employees, prospective school employees, contractors, parents, students and volunteers of the School are responsible to be familiar with and abide by this policy.

5. Related Documents

- *Privacy Act 1988* (Cth)
- *Health Records Act 2001* (Vic)
- *Surveillance Devices Act 1999* (Vic)
- *Children's Services Act 1996* (Vic)
- *Children's Services Regulations 2009* (Vic)
- Australian Privacy Principles — a summary for APP entities, OIAC, 2014
- Privacy Compliance Manual, CEC and ISC as updated from time to time
- Recruitment and Selection Policy
- Register of Personal Information Collected by IGS
- Permission to Use Student Images
- Counselling Disclosure Statements to Students
- Privacy Alumni Collection Notice
- Privacy Employment Collection Notice
- Privacy Contractor/ Volunteer Collection Notice
- Privacy Standard Collection Notice

6. Definitions

Australian Privacy Principals (APPS) are defined by the Privacy Act and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information;
- an organisation or agency's governance and accountability;
- integrity and correction of personal information; and
- the rights of individuals to access their personal information.

Data Breach means when personal information is accessed, disclosed without authorisation, or is lost. For example:

- loss of a mobile phone or computer with personal information;
- accidentally sending an email with personal information to people who it was not meant for; or
- disclosing medical information to people who did not need to see it.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Examples include an individual's name, address, contact number and email address.

Sensitive Information is a special category of Personal Information and means:

- information or an opinion about an individual's:
  - racial or ethnic origin; or
  - political opinions; or
  - membership of a political association; or

- religious beliefs or affiliations; or
- philosophical beliefs; or
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual preferences or practices; or
- criminal record;

- that is also personal information; or
  - health information about an individual; or
  - genetic information about an individual that is not otherwise health information; or
  - biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
  - biometric templates.

Last review date: August 2020	Approved by: Principals Executive
Next review date: August 2022	Approval date: August 2020
Policy owner: Privacy Officers	