

Student Privacy Policy

Policy Category	Corporate		
Policy Owner	General Manager IGI		
Responsible for Implementation	Registrar		
Review Date (2 years)	October 2025		
Relevant to	IGI Students		
Related Documents	Student Record Management Policy Staff Code of Conduct		
Version	Authorised by	Approval Date	Effective Date
1.1	General Manager IGI	1 Oct 2023	1 Oct 2023

1. Purpose

The Privacy Policy specifies the principles guiding the management of personal information and safeguarding of student privacy at IGI. This policy provides an overview of the personal information handling practices, procedures, and systems. It also provides guidance to staff in relation to the creation, management, storage, retrieval, and disposal of student personal records.

The requirements for privacy have been set and approved by IGI governing bodies to ensure that IGI manages personal information transparently and responsibly, and complies with relevant legislative and regulatory standards as well as good practice principles in the management of personal information.

2. Definitions

Definitions	
Disclosure of Information	Refers to the communication or transfer of information outside IGI.
Health information	Personal information that is information or an opinion about the physical or mental health or a disability (at any time) of an individual
Personal information	Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion
Sensitive information	A subclass of personal information that has higher level of privacy protection than other personal information. It can relate to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual orientation, criminal record, etc.
Staff	All employees of IGI, including permanent and casual employees, consultants and contractors, education agency staff, committee members and any other person appointed or engaged by IGI to perform duties or functions for IGI
Use of Information	Communication or handling of information within IGI.

3. Scope

This policy applies to prospective and enrolled students and staff handling personal information.

4. Policy statement

- 4.1. IGI is committed to keeping personal information private and secure.
- 4.2. IGI only collects personal information that is necessary to conduct its business as a higher education provider.
- 4.3. IGI will never rent, trade, or sell personal information to a third party.
- 4.4. IGI will never publicly display personal details that identify you without prior consent.

5. Principles

- 5.1. IGI is committed to the following principles that underpin this policy:
- 5.2. IGI fosters a culture of respect of privacy to reduce invasiveness, as far as practicable.
- 5.3. IGI regularly reviews its activities and considers whether it is necessary to collect and hold personal information in order to carry out the specific functions or activities.
- 5.4. IGI embeds privacy protections into the design of information handling practices.
- 5.5. IGI maintains the quality of personal information that is used and disclosed.
- 5.6. IGI only discloses student information with the consent of the student or only do so if the student would expect it, or where legally required to do so.
- 5.7. IGI regularly conducts activities to identify, assess and manage privacy and security risk, as well as develops and monitors controls for those risks.

6. Collection of personal information

Purposes

- 6.1 IGI collects information for the following purposes:
 - admission, including assessment of a prospective student's capacity to participate and progress in a course of study offered at IGI;
 - administration, including transactions relating to fees;
 - safety and security, including through monitoring IT activity and security cameras;
 - equal opportunity measures, including reasonable adjustments and disability support;
 - advice on access to support services;
 - complaints and appeals processes, including investigation into potential breaches of the Student Code of Conduct or academic integrity;
 - quality improvement, e.g. of the student experience, educational offerings, curriculum, or support services;
 - authentication of graduation certification;
 - alumni program; and
 - any legislative or regulatory obligations.
- 6.2 As far as possible, IGI will use de-identified data, in particular for quality improvement purposes (e.g. for monitoring trends and taking remedial action, etc.).

- 6.3 IGI will offer the option to students to remain anonymous where possible, such as when responding to surveys.
- 6.4 Staff members receive privacy training during induction and are aware of the potential adverse consequences of unnecessary invasiveness and of privacy breaches.

Types of personal information

- 6.5 IGI collects and holds a large variety of personal information relating to the whole student lifecycle at IGI, from prospective students to alumni. This information includes but is not limited to:
- full name, date of birth, gender, contact details, billing address, tax file number, passport document number, bank account number, driver's licence number, emergency contacts, details of next of kin;
 - all applications, including admission, special consideration, reasonable adjustment, review of assessments;
 - information relating to enrolment, including variation to enrolment;
 - assessment results, academic transcripts, testamur, and attainment records;
 - breaches of the Student Code of Conduct or academic misconduct, including sanctions and penalties;
 - information relating to complaints and appeals; and
 - health and sensitive information, such as collected by Student Services.

7. Personal information handling

Collection

- 7.1 IGI will collect personal information through a variety of methods, including online forms, direct interaction with staff members, security cameras, network use, or audio and video recordings of events.
- 7.2 IGI will take steps to ensure that students are appropriately notified where personal information is collected.

Storage

- 7.3 All students are allocated an individual file upon formal application for enrolment at IGI. The student file contains at a minimum:
- application and certification documentation, enrolment data, financial transactions, academic results, formal communications between staff and students; and
 - external communications about students that are generated by IGI.
- 7.4 As a rule, in determining appropriate storage, consideration will be given to the protection provided by any selected storage facility, sensitivity of records, required retention periods as well as access requirements and demands.
- 7.5 Staff members are instructed not to relinquish, amend, destroy or damage records containing personal information without approval.
- 7.6 IGI implements measures for ensuring the quality of data that is collected, held, and disclosed by IGI, including training for the collection of data, and verification and validation protocols.

Security

- 7.7 IGI takes reasonable steps to protect personal information from misuse, interference, loss, and from unauthorised access, modification, or disclosure.
- 7.8 IGI is aware of the possible adverse consequences that a privacy breach would have on both students and IGI and maintains a current understanding of the variety of risks it faces, including common threats and vulnerabilities.
- 7.9 IGI conducts regular privacy impact assessments, information security risk assessments and reviews of personal information security controls in accordance with the Risk Management Policy. IGI ensures that risk assessments are conducted following significant changes to organisational structure, technological systems, or legislative requirements.
- 7.10 IGI provides training and regular refreshers on physical and IT security and the handling of personal information to permanent and casual staff and contractors. The training includes information on the importance of not accessing personal information or databases unnecessarily, what would constitute misuse of personal information, identity authentication procedures, and on recognising and avoiding inadvertent disclosures when for example verifying students' identity or publishing information on IGI's website or learning management system.
- 7.11 Other security controls include: regular review of rights to access to personal information, revocation of such access when staff leave the organisation or change roles, protocols for the printing of documents containing personal information or for the security of physical files while working from home or other site, application of labels with IGI's contact details on mobile devices in case of loss, and use of remote wiping software to allow for the deletion of personal information stored on devices which have been lost or stolen.
- 7.12 IGI ensures the adequacy of security protections of its systems with its suppliers, including by ensuring the use of measures such as anti-virus, firewall, continuous monitoring of servers for possible attacks, regular patches and updates, encryption of data, authentication of users, encryption of login details, and regular and multiple back-ups of data.
- 7.13 IGI implements strategies to eliminate or mitigate:
- human error risk by raising awareness of staff during induction, and providing regular updates, on common social engineering techniques; and
 - trusted insider risk by monitoring access to systems hosting personal information and regularly reviewing audit logs.

Disclosure by IGI

- 7.14 IGI will not disclose a student's personal information unless:
- the student is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person or organisation;
 - the student has given written consent to the disclosure;
 - IGI believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the student or of another person;
 - the disclosure is required or authorised by or under law; or
 - the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
- 7.15 IGI may disclose personal information to Australian Government agencies and relevant authorities, such as the Department of Home Affairs, Department of Education, Australian Taxation Office, relevant Overseas Student Health Care Providers, Federal and State Police, or the Tuition Protection Service.

- 7.16 IGI will disclose personal information to third parties in the course of a student's course, such as an industry partner for a placement, support services, or health services. In those instances, IGI will ensure that only necessary personal information for the purpose of the placement or service is disclosed.
- 7.17 IGI enters into agreements with third parties which include provisions to ensure compliance with privacy laws.
- 7.18 IGI may disclose personal information to overseas recipients, especially with regard to international students. IGI will only provide this information as per the above disclosure principles, where it has established an agreement which would ensure compliance with Australian privacy laws, or where IGI thinks the recipient is subject to laws which are substantially similar to the Privacy Act 1988.

Access and correction by students

- 7.19 IGI will provide a student with access to their personal information when requested by the student and if the identity of the student has been established. A student need not provide a reason for requesting access to their personal information.
- 7.20 IGI takes reasonable steps to ensure that the personal information it holds is accurate, up-to-date, complete and relevant, and will correct personal information when requested by the student, having regard to the purpose for which it was collected.
- 7.21 All requests for access to personal information must be directed to the General Manager IGI (or delegate) by email or in writing.
- 7.22 In some cases, IGI may refuse to give access to personal information. This may include circumstances where giving access would:
- be unlawful, e.g. where a record that contains personal information is subject to a claim for legal professional privilege by contractual counterparties;
 - have an unreasonable impact on another person's privacy; or
 - prejudice an investigation of unlawful activity.
- 7.23 IGI will provide reasons for any refusal to give access to personal information.

Disposal

- 7.24 Student file records are retained and disposed securely in accordance with the Records Management Policy.
- 7.25 IGI regularly reviews personal information it holds to determine if the information is no longer needed.
- 7.26 Staff may not destroy records containing personal information without approval.
- 7.27 IGI also takes reasonable steps to destroy or de-identify personal information once it is no longer needed. Destruction of personal information ensures that it is irretrievable or, if not possible, puts the data beyond use.

Data breaches

- 7.28 IGI notifies affected individuals and the Australian Information Commissioner in the event of a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

8. Roles and responsibilities

- 8.1 The Governing Board:
- approves the Privacy Policy; and
 - receives reports about the effectiveness of processes for the management of personal information and the integrity of the systems on which it is stored.
- 8.2 The Executive Management Team is responsible for monitoring and making recommendations for improvement relating to privacy matters.
- 8.3 The General Manger IGI (or delegate) is the owner of this policy and is responsible for:
- issuing regular communications on the importance of safeguarding personal information;
 - acting as IGI’s Privacy Officer; and
 - monitoring staff access and permissions relating to personal information.
- 8.4 The Registrar is responsible for the implementation of this policy.

9. References

- Higher Education Support Act 2003
- Education Services for Overseas Students Act 2000
- Higher Education Standards Framework (Threshold Standards) 2021
- National Code of Practice for Providers of Education and Training to Overseas Students 2018
- Tertiary Education Quality and Standards Agency Act 2011 Commonwealth Education Services for Overseas Students Act 2000
- Privacy Act 1988

10. Document History

Version	Date	Author	Reason	Sections
1.0	Jun 2022	PBL Education	New policy	All
1.1	Oct 2023	IGI	Rebrand and minor amendments	All