Personal Information and Privacy Policy and Procedure

Purpose

1. Queensland Institute of Higher Education ('the Institute') recognises that privacy is a fundamental human right and that the Institute has responsibilities and obligations when handling personal information.
2. This Policy provides an overview of the personal information held by the Institute, and personal-information-handling practices, procedures and systems. It also provides guidance to staff of the Institute in relation to the creation, management, storage, retrieval, and disposal of personal records. This Policy complies with relevant legislative and regulatory standards as well as good practice principles in the management of personal information.

Scope

3. This Policy applies to:
   a) all prospective and enrolled students and alumni of the Institute;
   b) all staff of the Institute whether full-time, part-time, casual or contract;
   c) members of the Institute's Governing Bodies.
   d) all personal information held by the Institute including paper-based and electronic records;

Definitions

4. For the purposes of this Policy:
   a) ***Personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable, including a person's name and address, medical records, bank account details, photos, and videos.
   b) **Sensitive information** means personal information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, sexual orientation or practices, criminal record, health information,
   c) ***Records:*** a record is any information captured by hard copy, technological or electronic means that pertains to the Institute and its community.
   d) ***Secure records:*** the security of records is established through electronic back-up, and/or secure storage on-site or off-site in an area where records are protected from damage and incursion but may be retrieved as required and authorised.
   e) ***Student records:*** records in paper-based or electronic format that capture data pertaining to the student journey including records of application, enrolment, academic progress, departmental interactions, and graduation.

Policy

Statement

5. The Institute recognises that it deals with personal, often sensitive, information about individuals on a daily basis and that it has a responsibility to preserve and protect personal information. The Institute is committed to good practice in management of personal information by implementing this Policy.

Principles

6. When handling personal information, the Institute will:
   a) foster a culture of respect of privacy to reduce invasiveness as far as practicable;
   b) regularly review its activities and consider whether it is necessary to collect and hold personal information in order to carry out the specific functions or activities;
   c) embed privacy protections into the design of information-handling practices;
   d) maintain the quality of personal information that is used and disclosed;
   e) only disclose 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;
   f) regularly conduct activities to identify, assess and manage privacy and security risk, as well as develop and monitor controls for those risks.

Procedure

Purposes for collecting personal information

7. The Institute collects information for the following purposes:
   a) admission, including assessment of the student's capacity to participate and progress in a course offered at the Institute;
   b) administration, including transactions relating to fees;
   c) human resource management;
   d) safety and security, including through security cameras;
   e) equal opportunity measures, including reasonable adjustments and disability support;
   f) advice on access to support services;
   g) grievance and appeals processes, including investigation into potential breaches of relevant codes of conduct and policies;
   h) quality improvement, e.g. of the student or staff experience, educational offerings, curriculum, or support services;
   i) authentication of graduation certification;
   j) alumni network; and
   k) any legislative or regulatory obligations.
8. As far as possible, the Institute will use de-identified data, in particular for quality improvement purposes (e.g. for monitoring trends and taking remedial action, etc.).
9. The Institute will offer the option to staff and students to remain anonymous or to use a pseudonym where possible, e.g. when responding to surveys.

10. 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

11. The Institute collects and holds a large variety of personal information relating to the whole student lifecycle at the Institute, from prospective students to alumni and to all staff. This information includes:
    a) 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;
    b) all employment and related human resource records;
    c) breaches of codes of conduct or other policies, including sanctions and penalties;
    d) information relating to grievances, complaints and appeals;
    e) health and other personal information, e.g. as collected by Student Services or supervisors;
    f) for students, specific enrolment- and course-related information such as:
        i. all applications, including admission, special consideration, reasonable adjustment, review of assessments;
        ii. variations to enrolment;
        iii. assessment results, academic transcripts, testamur and attainment records.

Collection

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

Storage

14. All students are allocated an individual file upon formal application for enrolment at the Institute. The student file contains at a minimum:
    a) application and certification documentation, enrolment data, financial transactions, academic results, formal communications between staff and students; and
    b) external communications about students that are generated by the Institute.
15. All staff are allocated an individual file on appointment to the Institute which contains all recruitment and employment-related records including outcomes of performance reviews, applications for leave with accompanying evidence, and any information gathered as part of any investigation into any allegations, grievances or appeals.
16. As a rule, in determining appropriate storage, consideration must be given to the protection provided by any selected storage facility, sensitivity of records, required retention periods as well as access requirements and demands.
17. Staff members are instructed not to relinquish, amend, destroy or damage records containing personal information without approval from the Chief Executive Officer (CEO) or Chair of the Governing Council. The *Authority Delegation Policy* outlines applicable delegated authorities for the handling of personal information.

18. The Institute implements measures for ensuring the quality of data that is collected, held and disclosed by the Institute, including training for the collection of data, and verification and validation protocols.

Security

19. The Institute takes reasonable steps to protect personal information from misuse, interference, loss, and from unauthorised access, modification or disclosure.
20. The Institute is aware of the possible adverse consequences that a privacy breach would have on all stakeholders and the Institute and maintains a current understanding of the variety of risks it faces, including common threats and vulnerabilities.
21. The Institute conducts regular privacy impact assessments, information security risk assessments and reviews of personal information security controls in accordance with its *Risk Management Policy*. The Institute ensures that risk assessments are conducted following significant changes to organisational structure, technological systems, or legislative requirements.
22. The Institute provides training and regular refreshers on physical and ICT 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 the Institute's website or Learning Management System.
23. 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 the Institute'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.
24. The Institute 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.
25. The Institute implements strategies to eliminate or mitigate:
    a) human error risk by raising awareness of staff members during induction, and providing regular updates, on common social engineering techniques; and
    b) trusted insider risk by monitoring access to systems hosting personal information and regularly reviewing audit logs, such as:
        i. limiting access to personal information to those staff necessary to enable the Institute to carry out its functions;
        ii. number of users with administrative privileges limited to staff requiring those privileges;
        iii. physically disabling USB or other external port access to devices or disabling internal CD/DVD writers on devices of staff with access to sensitive information.

Disclosure by the Institute

26. The Institute will not disclose an individual's personal information unless:
    a) the individual is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person or organisation;
    b) the individual has given written consent to the disclosure;
    c) the Institute 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 individual
    d) the disclosure is required or authorised by or under law; or
    e) 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.

Government agencies

27. The Institute may disclose personal information to Australian Government agencies and relevant authorities, such as the Department of Home Affairs, Department of Education, Skills and Employment, Australian Tax Office, relevant Overseas Student Health Care Providers, Federal and Queensland Police, or the Tuition Protection Service.

Third parties

28. The Institute will disclose student personal information to third parties in the course of a student's course, such as a work-integrated learning host organisation, support services, or health services. In those instances, the Institute will ensure that only necessary personal information for the purpose of the placement or service is disclosed.
29. The Institute enters into agreements with third parties which include provisions to ensure compliance with privacy laws.

Overseas recipients

30. The Institute may disclose personal information to overseas recipients, especially with regard to international students. The Institute 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 the Institute thinks the recipient is subject to laws which are substantially similar to the *Privacy Act 1988*.

Access and correction by individuals

31. The Institute will provide an individual with access to their personal information when requested by the individual and if the identity of the individual has been established. An individual need not provide a reason for requesting access to their personal information.
32. The Institute 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 individuals, having regard to the purpose for which it was collected.

Disposal

33. Personal records must be retained and disposed of as outlined in the *Records Management Policy and Procedure*.
34. The Institute will regularly review personal information it holds to determine if the information is no longer needed.

35. Staff members may not destroy records containing personal information without approval from the CEO or Chair of the Governing Council. The *Authority Delegation Policy* outlines relevant delegated authority for the handling of student information.
36. The Institute also takes reasonable steps entities to destroy or de-identify personal information once it is no longer needed. Destruction of personal information will ensure that it is irretrievable or, if not possible, puts the data beyond use.

Breaches of Australian Privacy Principles

37. The Institute is required to notify affected individuals and the Australian Information Commissioner in the event of 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates. The Institute conducts a prompt and reasonable assessment if they suspect that they may have experienced an eligible data breach.
38. Where a member of staff becomes aware of, or suspects, a data breach, the Privacy Officer must be notified of this. The report should include a description of the breach: time and date of the incident or discovery of the breach, type of breach (i.e. unauthorised access or disclosure, or loss), type of information involved in the breach, likely cause of the breach, and any action taken to mitigate the impact of the breach. The Privacy Officer must keep a record of the incident report.
39. The Privacy Officer will assess whether the breach involves personal information and the severity of the breach, taking into account the sensitivity of the information, volume of data involved in the breach, and risk of harm to individuals.
40. The Privacy Officer will coordinate a response to the breach in consultation with the CEO. Depending on the extent of the breach, the Privacy Officer may form a response team, which will be composed of the Executive Management Team members and other staff as required. The Privacy Officer will ensure that immediate remedial action takes place to contain the breach and prevent further breaches. This could include:
    a) for unauthorised access:
        i. reset access details and passwords of compromised devices and systems;
        ii. isolate compromised devices and systems;
        iii. shut down compromised devices and systems;
    b) for unauthorised disclosure:
        i. request unintended recipients to delete the email;
        ii. remove the information from the internet or intranet website where it was published;
    c) for data loss:
        i. disable device remotely;
        ii. search and retrieve lost files or folders.
41. Where the incident is an eligible data breach, the Privacy Officer will notify the Office of the Australian Information Commissioner, including a description of the data breach, the kinds of information involved, and recommendations about the steps individuals should take in response to the data breach. The CEO will inform the Governing Council of the breach and the institutional response to the breach.

42. The Privacy Officer will notify the affected individuals, including actions taken by the Institute to mitigate the breach and prevent further breaches, steps that they can take to reduce the risk that they experience serious harm as a result of the breach, and that the Office of the Australian Information Commissioner has been notified of the matter (as applicable).
43. The Privacy Officer will review the incident, consider what actions can be taken to prevent future breaches, discuss with the Executive Management Team, and report on the matter to the Audit and Risk Committee and ultimately to the Governing Council with proposed improvements.

Complaints

44. Complaints relating to personal information may be addressed under the provisions of the *Student Grievance Policy and Procedure* or the *Human Resources Management Policy and Procedure*.

Responsibilities

45. Personal information is the overall responsibility of the CEO and the Governing Council.
46. The Student Services Manager is the nominated Privacy Officer for the Institute. The Privacy Officer is responsible for managing compliance with Australian privacy laws, conducting privacy impact assessments and coordinating the Institute's response to data breaches.
47. The Student Services Manager is responsible for the management of student records.
48. All student information handling processes must comply with this Policy and training will be undertaken as part of all staff induction.

Associated information

Approving body	Governing Council
Date approved	23 October 2020
Date of effect	Commencement of operation
Next scheduled review	Two years from when policy commence
Policy owner	Chief Executive Officer
Policy contact	Chief Executive Officer
Related AIIHE Documents	*Authority Delegation Policy* *Quality Assurance Framework* *Records Management Policy and Procedure*
Higher Education Standards Framework (Threshold Standards) 2015 (Cth)	Standard 2.4, ss 4 Standard 7.3, ss 3
Other related external instruments/documents	**Related Legislation** • *Tertiary Education Quality and Standards Agency Act 2011 (Cth)* • *Education Services for Overseas Students Act 2000 (Cth)* • *National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth)* • *Privacy Act 1988 (Cth)* **Good Practice Documents** • *Office of the Australian Information Commissioner: Data breach preparation and response. A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*

Document history

Version	Author	Changes	Approval Date
1.0	Not applicable	Original version	23 October 2020

Warning - Document uncontrolled when printed! The current version of this document is maintained on the AIIHE website at www.aiihe.edu.au