Personal Information Privacy Plan

In pursuit of its vision and mission, the University is committed to:

- rigorous standards of scholarship
- positively influencing our communities through our teaching, research and scholarly activities
- recognising our location in the Asia-Pacific and deepening our engagement with the region
- bringing disciplines together to address the key issues of our time
- promoting the respect of individual rights and ethical standards
- participatory decision making and problem solving
- contributing to a robust, equitable and environmentally sustainable society
- recognising and valuing diversity
- recognising the unique place of First Peoples in Australian history and culture, and enabling their continued contribution to the nation.

The University's commitment to individual rights, ethical standards and sustainability includes commitments to the appropriate collection, storage and use of information, and to the protection of the privacy of personal information. The Griffith Information Management Framework requires that data and information be secured and protected from unauthorised access, use and disclosure.

In undertaking our normal business of teaching, learning and research, the University collects, stores and uses personal information. Learning and research in all fields of human endeavour will often necessarily involve the collection of personal information. While we treat this information with the highest standards of security, confidentiality and privacy, there are occasions when we may disclose this information to third parties where required by law, or where necessary for the conduct of our business.

There are a range of guidelines, processes and policies already in place to protect the privacy of personal information at Griffith University. This Privacy Plan represents the integration of the Information Privacy Principles (IPP), set out in the *Information Privacy Act 2009*, schedule 3, into the University's existing policy framework, and is the umbrella instrument for all documents relating to confidentiality and privacy within the University.

The overall responsibility for privacy in the University resides with the Vice Chancellor and President. University Council has delegated the authority to approve or not approve changes to the University's Privacy Plan to the Vice Chancellor as the Principal Officer under the *Information Privacy Act 2009*. The responsibility for day to day management has been delegated to the Vice President (Corporate Services). The Vice President (Corporate Services) as Privacy Contact Officer is the first point of contact for members of the campus community and the public on privacy matters including general information, requests to access and/or amend personal information, and for internal review and resolution of complaints.

The contact details for the Privacy Contact Officer are as follows:

The Privacy Contact Officer
Office of the Vice President (Corporate Services)
Griffith University
Nathan Qld 4111
Facsimile: +61 07 373 57507
Email: vpcorporateservices@griffith.edu.au

Legislative Requirements

The Griffith University Privacy Plan has been developed in accordance with the Information Privacy Principles (IPP) set out in the *Information Privacy Act 2009*, schedule 3. These IPPs represent the community standard for collecting, storing, using and disclosing personal information by public agencies in Queensland. The Queensland IPPs are similar to the National Privacy Principles set out in the *Privacy Act 1988 (Cth)*, schedule 3.

The *Right to Information Act 2009* and the *Information Privacy Act 2009* replaced Freedom of Information (FOI) laws and are designed to provide appropriate safeguards for the way the public sector handles an individual's personal information.

Personal Information

Personal information is defined as information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Records generally relate to current and former staff and students and may be stored on a variety of media including paper and electronic databases, photographic and video image, digital form and may also extend to body sample and biometric data.

The University collects, stores and uses personal information to administer a variety of business related and administrative programs. Appendix 1 provides a comprehensive list of the types of personal information the University collects. Individuals can obtain information regarding access to their personal information documents under the provisions of the *Information Privacy Act 2009* by contacting the Privacy Contact Officer. Records may relate to persons with a current, former or future relationship with the University.

In general, the University will not use or disclose personal information unless the person about whom the information was collected is aware of, or has consented to that use of disclosure. However, the University may use or disclose personal information where required by law, or where it is necessary for certain types of law enforcement, or where it is necessary to protect against a serious and imminent threat to a person's life or health.

The University's email, calendar and associated web-based application systems (for example Google docs) are a 'cloud based' system. Data in these systems, which may include personal information and attachments, is hosted by third parties off-shore in a range of jurisdictions. The exact location of this data may change from time to time and it is not practicable to specify the countries in which that data will be hosted.

The University will assess unsolicited personal information given to it and delete or de-identify that information, unless it is relevant to or reasonably necessary for the University's functions or purposes.

Any staff member who becomes aware of a data breach involving personal information must report that data breach to the Privacy Contact Officer.

List of Public Registers Managed Within Griffith University
Griffith University is not required to maintain any public registers. Any person who believes that there is a public register maintained either by or within the University that may affect them adversely should contact the Privacy Contact Officer.

Procedure to Gain Access to Personal Information
Individuals can obtain information about personal information which the University may hold about them, and can request access to that information by writing to the Privacy Contact Officer. Individuals can also write to request an amendment to the personal information held by the University about them, or to request an internal review of a decision made in response to a request for access or amendment. For further information, see Procedures for Access to and Amendment of Personal Information/Complaints and Internal Review Procedures.

Review Procedure
If an individual believes that their personal information has not been dealt with in accordance with an IPP they may make a written complaint to the Privacy Contact Officer. Requests should be made as soon as possible from the date when the breach was suspected to have occurred.

Requests will be acknowledged in writing within 14 days from the date on which the application was received, and the University will process the request within 60 days from the date on which the application was received. Applicants will be advised in writing of the University's decision.

If an individual does not agree with the decision of the Privacy Contact Officer, they may request an internal review by writing to the Vice Chancellor and President. The Vice Chancellor and President will arrange for an internal review to be carried out by a senior officer who has not previously been involved in the matter. This will be done within 45 days. The applicant will receive a response in writing.

Where a person remains dissatisfied with the outcome of an internal review process, the person may make a privacy complaint to the Office of the Information Commissioner provided at least 45 business days have elapsed since the complaint was made to the Privacy Contact Officer.

Alternatively, an individual may make a privacy complaint to the Office of the Information Commissioner without requesting an internal review provided at least 45 business days have elapsed since the complaint was made to the Privacy Contact Officer.

For further information, see Procedures for Access to and Amendment of Personal Information/Complaints and Internal Review Procedures.

Ian O'Connor
Vice Chancellor & President