

UNIVERSITY OF MELBOURNE

Privacy Statement for Staff Information

Privacy Legislation

The University of Melbourne complies with the provisions of the Information Privacy Act 2000 (Vic) and the Health Records Act 2001 (Vic) in its treatment of personal and health information (referred to collectively in this document as personal information).

What we collect and how

• Personal Information

The University will collect personal information about you during the course of your employment. Such information may include your name, date of birth, address, tax file number, banking details, superannuation details, qualifications, performance appraisals, details of paid outside work /directorships and referee reports and other information.

The information is often collected from several sources. For instance, you provide us with information when you complete employment forms and when you enter data directly into our computerised HR system. Other people such as previous employers and nominated referees may also provide us with information about you.

All HR forms and processes that collect personal information will have a reference to the University's Privacy web site and to this statement

• Health Information

Health information is often collected when you commence work as part of the University's occupational health and safety monitoring. A brief medical/vaccination history is requested in order to identify any areas where there could be a health or hazard risk. The information is assessed and then stored by the Occupational Health Service within Human Resources. On receipt of a written request, the information may be provided to our Environment Health and Safety Office, where it is required to manage or administer a work cover issue.

Why we collect the information

The primary purpose for collecting the information is to maintain your employee records and to administer your employment, salary and superannuation. Your personal information may also be used in other related Human Resources processes and in an aggregate (non-identifying) form to report on workforce profiles and where required, to external bodies.

Accuracy, Security and Storage of Information

The University holds personal information in computer and paper based records. It takes all reasonable steps to ensure that the personal formation it holds is accurate and complete and that it is protected from misuse, loss, unauthorised access or disclosure.

Disclosure of Information

The University will only disclose information as required or permitted by law, or with your consent.

Access to personal information

You have direct access to your personal information unless it is deemed that providing you with access would have an unreasonable impact on the privacy of others. Otherwise, access to and correction of personal information is handled in accordance with the Freedom of Information Act 1982. Applications for access under that Act should be addressed to the Senior Vice-Principal.

Job Applications

Information provided by job applicants is used solely for the purpose of the recruitment function. The information is disclosed only to staff and/or relevant panel members involved in the selection process, and will remain confidential. As a general rule, the University keeps an electronic copy of all job applications and these are disposed of six months after the recruitment process is completed.

University Privacy Officer/ Privacy Policy

The University's Privacy Officer is the University Secretary, Dr Christopher Stewardson. The Privacy Officer's website at <http://www.unimelb.edu.au/unisec/privacy/> contains the University's Privacy Policy and provides detailed information about the contact details, complaints procedures and other aspects of the University's privacy regime.

Questions

If you have an enquiry about your privacy rights in relation to the collection of information please contact the University's Privacy Officer at privacy-officer@unimelb.edu.au

Use of University IT Facilities

When you use University IT facilities, your identity is usually ascertainable by the University and University systems keep logs of things like logging in and out, visits to web pages, emails sent or received using University email systems. In general, these logs are used in the course of managing the facilities, for things like fault rectification and performance tuning. They may also be used in the course of authorised investigation into IT security matters, or authorised disciplinary investigations. Staff are not permitted access to the logs except to the extent necessary to perform their duties. Information may be disclosed to third parties if we are required or authorised to do so by law. Email sent or received by staff in the course of University duties may be subject to Freedom of Information requests.