

Recruitment and Employment Privacy Notice



This privacy notice outlines how your personal information is managed throughout The University of Melbourne's (**University**) recruitment and employment process. It should be read in conjunction with the University's [Staff Privacy Statement](#), the University's [Recruitment and Appointment Policy](#) and [Appropriate Workplace Behaviour Policy](#). Other [employment policies and procedures](#) can be found in our Policy Library and a copy of the [University's Enterprise Agreement](#) is available on the Fair Work Commission website.

Why we collect your personal information

The University collects and processes your personal information to:

- assess and process your application for employment with the University
- conduct necessary pre-employment screening checks and onboarding processes
- maintain your employee records and administer your employment, salary and superannuation
- maintain up to date information in our recruitment and employment relationship systems
- meet our legislative obligations in accordance with the *Fair Work Act 2009* (Cth), State and Federal equal opportunity and anti-discrimination legislation, the *Child Employment Act 2003* (Vic), the Higher Education Standards Framework (HESF), and the *Occupational Health and Safety Act 2004* (Vic)
- comply with other workplace and employment laws, including State and Federal safety and security laws requiring background checks and ongoing record keeping, and for mandatory government reporting purposes
- inform general business analysis, quality assurance, reporting and planning activities

The "processing" of personal information refers to all activities relating to the management of your personal information, from its collection and use, through to its storage and disposal, and everything in between.

How we process your personal information

We will process your personal information as necessary to support our legitimate interests, in accordance with applicable privacy laws, and only under the following circumstances:

- for the purpose for which it was collected; or
- a related purpose which you might reasonably expect; or
- where you have consented to the processing; or

- if we are required or permitted to do so by law.

We will only process your health or sensitive information, as defined in relevant privacy legislation, with your consent or where required or permitted to do so by law.

Wherever possible, we will collect your personal information directly from you. For example, you provide us with information when completing employment forms and when entering data directly into our Human Resources and other systems, during the application and recruitment process, and once you are employed or engaged by the University. However, where this is not reasonable or practicable, we may collect information indirectly or automatically for specific purposes. These include:

- engaging third-parties to undertake pre-employment screening and checks, such as for visa sponsorship, including guests, honoraries and visitors;
- enquiries and activities relating to workplace or misconduct investigations during your employment, where information may be provided by other staff, students, or relevant third parties, or sourced from publicly available information, including social media;
- data collected via the University's wireless network (**UniWireless**) to inform space utilisation and campus management, to develop and refine estate services and support, and to investigate and regulate compliance with the conditions of use and University regulations and policies. The University's [Wireless Terms of Use](#) provide more information;
- data collected when you access University property and facilities, for the purposes of maintaining a safe and secure campus, managing traffic and infrastructure, and assisting in access to controlled environments. This includes Security Safety System footage (formerly known as CCTV), building access records, body-worn camera recordings and other mobile device recordings;
- data automatically collected from you when you visit websites controlled by The University of Melbourne, such as through the use of cookies and similar technologies, as detailed in our [Online Privacy Statement](#);

In addition, use of University IT and facilities may be logged, monitored, recorded and analysed by authorised staff to substantiate an allegation of misuse or to facilitate the investigation of an activity that may be contrary to University regulations, policy, or the law, including activities unrelated to network or facility use. Such information may be used for the purposes of misconduct and disciplinary processes and may on occasion include wireless network connection data, building access data, and information contained in University-allocated email accounts (which are provided for work-related purposes). This accords with the University's [Wireless Terms of Use](#), [Provision and Acceptable Use of IT Policy](#), [Property Policy](#) and [Appropriate Workplace Behaviour Policy](#).

Your personal information may be processed in various ways, depending on the nature of your interaction with the University, as described in the following table. If you choose not to provide the information requested, we may be unable to assess your employment application, or administer your employment, or it may limit the benefits and assistance available to you.

Interaction with the University	Data collection and purpose	Use and disclosure
Recruitment, application and selection	Your personal data is requested to assess and process your application for employment with the University. Information you provide as part of your application includes: • your name and contact details • details of your education and/or previous employment • your qualifications and details of professional memberships • your responses to selection criteria and/or interview questions • your nominated referees • your residency or visa status, if applicable, to demonstrate your work rights in Australia • other demographic data, such as Aboriginal/Torres Strait Islander status, where relevant • information for reasonable adjustments and accessibility to allow candidates to participate in the interview and recruitment process, where relevant	Information provided by job applicants is processed in secure University systems and is used solely for the purposes of recruitment and selection and to form the basis of the employment record of successful candidates subsequently employed. It is treated confidentially and only disclosed to hiring managers, relevant panel members, and/or other staff involved in the selection process and the administration of HR functions. Your information may also be disclosed to third parties engaged by us to support and administer our HR systems and processes. The personal information of job applicants is only retained for as long as it is required for the purpose it was collected and is then securely destroyed in accordance with the University's legislative obligations and our Retention and Disposal authority.
Accepting an offer, pre-employment checks and declarations	Information you provide as part of our onboarding and engagement process is used for the purposes of undertaking pre-employment checks, making an offer of employment, processing your acceptance of any offer, and onboarding you as an employee. It forms the basis of an individual's employee record upon confirmation of employment.	During recruitment, we share information such as your Curriculum Vitae (CV), Employment Contract, and Visa Entitlement Verification Online check (VEVO) with external specialists engaged by us to undertake pre-employment screening and checks. Your information may also be disclosed to third parties engaged by us to support and administer our HR systems and processes.

	We use the information you provide to undertake pre-employment screening and checks and to administer our onboarding processes. This includes: • your name, date of birth, address and contact details • tax file number, banking and superannuation details • confirmation of qualifications, education and/or previous employment • referee reports from referees you nominate • confirmation of professional memberships • working with children and other occupational permits or registrations • emergency contact details Where you provide the University with the personal data of other individuals, such as your emergency contacts, you are encouraged to inform those parties that: • you are disclosing their data to the University; • their data will be retained in accordance with relevant University policies; and • their information can be accessed or amended by contacting HR Assist. If required by law, or where necessary for a particular position, we may conduct or require the following: • Criminal History Check • Bankruptcy Register search • Directorship search • Company check • Expanded International Sanctions lists check • Verification of registration with professional bodies and/or practicing certificates	The information of preferred and successful job candidates is processed in secure University systems and treated confidentially. It is only disclosed as necessary to hiring managers and staff involved in the pre-employment screening process and employment-related decision making, and those involved in the administration of HR functions. Your personal information is only retained for as long as it is required for the purpose it was collected and is then securely destroyed in accordance with the University's legislative obligations and our Retention and Disposal authority.
--	--	---

	• Background screening to comply with safety and security laws • Declarations and disclosures relating to export controls, sanctions, defence security, foreign interference, international collaboration and research conflict of interest We may also collect personal information about you from previous employers, other staff members and students, regarding your employment history and work. Before offering you a position, we (or agencies acting on our behalf) may collect information from third parties to conduct probity and background checks to determine your suitability for certain positions (for example through social media or other public sources in connection with our recruitment and human resources management processes).	
Employment	In addition to information collected during the offer and pre-employment stage, the University collects and processes your personal information throughout your employment. This information is required to administer your employment, salary and superannuation and maintain your employee records. The information is collected from several sources. For instance, you provide us with information when completing employment forms and when entering data directly into our HR and other systems. Other staff members, and students, may also provide us with information about your employment history and work-related matters where relevant to your employment.	Records relating to your employment are processed in secure University systems and treated confidentially. Access to employment information is limited to authorised staff involved in specific aspects of your employment relationship with the University. This includes: • staff responsible for administering your salary, superannuation, and any other benefits; • HR staff responding to your HR-related enquiries; • supervisors responsible for approving leave applications, work arrangements, and managing staff performance and development;

	The <i>Fair Work Act</i> requires us to keep certain personal information about employees in their employee records, including: • employee’s personal and emergency contact details • terms and conditions of employment • wage or salary details • leave balances and work hours • engagement, resignation or termination of employment • training, performance and conduct • taxation, banking or superannuation details • union, professional or trade association membership information. Other information collected throughout your employment includes: • performance appraisals • details of paid outside work or directorships • declared conflicts of interest • declared gifts, benefits or hospitality • disclosures and declarations relating to export controls, sanctions, defence security, foreign interference, international collaboration and research conflict of interest • other information relevant to your employment and work-related matters, including conduct and performance We may collect health information from you as part of the University's occupational health monitoring obligations and requirements.	• staff involved in workplace and misconduct investigations; and • staff responsible for Workcover investigations, occupational health monitoring, and occupational health and safety functions and obligations. Your information may also be disclosed to third parties engaged by us to support and administer our HR systems and processes and employment-related functions, including external specialists engaged by the University to undertake workplace and/or occupational health investigations. Where required, the University may share your information with external bodies such as the Australian Taxation Office, and other government departments or regulatory or law enforcement authorities, to meet mandatory reporting or disclosure requirements. Specific examples of when the University will disclose your personal data to third parties include for the following purposes: • to comply with a subpoena, summons, warrant, or other written order or notice from a government department, regulatory or law enforcement authority, court, or tribunal; • where disclosure is reasonably necessary to protect you or someone else from a serious threat to your or their life, health, safety, or welfare; • organisations that provide salary packaging benefits to eligible and participating staff members, where you are a participant staff member; and
--	--	---

	Health monitoring may be relevant where work performed has a significant risk to health because of exposure to a hazardous chemicals and substances, hazardous biological agents, radiation, noise or other occupational health hazards. We may collect and use your personal data including data collected from social media or other public sources to assist in the detection and investigation of actual or reasonably suspected misconduct, unlawful behaviour, or breaches of University regulations or policies. Such data and information is limited only to what is reasonably necessary for this purpose and access to this personal data is restricted to authorised personnel only.	insurance purposes, including the management of workers' compensation or work-related travel claims. Information collected from you for occupational health monitoring purposes may be disclosed to regulators in accordance with the University's legal obligations. Information relating to occupational health and safety incidents may also be disclosed in de-identified form internally with the relevant Occupational Health and Safety committee, the incident investigation team, and workers compensation team, or the manager of the relevant area involved. Your personal data may also be used for benchmarking purposes, analysis, quality assurance and workforce planning, and in an aggregate (non-identifying) form to report on workforce profiles. Your personal information is only retained for as long as it is required for the purpose it was collected and is then securely destroyed in accordance with the University's legislative obligations and our Retention and Disposal authority.
--	---	--

We may share your personal information with contracted service providers or partners engaged by us to perform legitimate functions on our behalf. For example, the University uses its business accounts under licencing agreements with third party platforms [Workday](#) (employee lifecycle), [Dayforce](#) (payroll), [Cayuse](#) (research administration), and [UKG](#) (time in attendance) to facilitate our human resource functions, including recruitment, workforce management, payroll and employee self-service. You can view their privacy policies to understand how they manage personal information.

In some instances, your personal information may be transferred outside of Victoria or Australia (for example, where providers are located internationally or use a cloud-based system with servers based in international jurisdictions). We take all reasonable steps to ensure that the interstate or overseas transfer of personal information is in accordance with our privacy obligations as outlined in the University's [Privacy Policy](#) and [General Privacy Statement](#).

Further privacy information

Refer to the [University's Privacy Statements](#) for general information about how we process and protect personal information, including:

- our lawful basis for processing personal information;
- collection, use and disclosure of personal information;
- accuracy, security and storage of personal information;
- retention and disposal of personal information;
- your individual rights; and
- applicable privacy laws.

The [University's Online Privacy Statement](#) outlines how personal information may be automatically collected from you, such as through the use of cookies, as a result of your visit to websites controlled by the University.

Your rights

You may request access to, or correction of, your personal information we hold, or exercise your individual rights as applicable under relevant privacy laws, unless this would have an unreasonable impact on the privacy of others or would contravene the University's other legislative obligations.

If the lawful collection of your personal information is based on your consent, you have the right to withdraw your consent at any time. However, this will not affect the lawfulness of our processing of your information prior to you withdrawing your consent.

Contact

For further information about Recruitment and Employment, you can contact us at hr-careers@unimelb.edu.au For information about how the University manages personal information, and for details of how to submit a privacy enquiry, lodge a privacy complaint, or to contact the University's Privacy and Data Protection Officer, please refer to our [Privacy webpage](#), view the [University's Privacy Policy](#) or contact privacy-officer@unimelb.edu.au.

Updates to this privacy notice

The University periodically refines its privacy notices to reflect appropriate information flows. The overall level of privacy protection is maintained when changes or inclusions are made. We will endeavour to inform you of any substantive changes; however, we may occasionally make changes without notice, particularly where there are changes in the relevant laws or we adopt new working practices. We therefore encourage you to regularly review this notice for any updates or to contact us for the most recent version.

Last updated: 19 August 2025