



Privacy Notice for Applicants, Employees and Workers

This privacy notice applies to all Southern Cross University (“the University”, “we”, “us”) job applicants, employees and workers including joint, visiting and adjunct academics, who provide the University with personal information in the course of their work at the University.

The information below sets out how the University handles personal information which is provided to the University in relation to the employment or working relationship.

The University's [Privacy Management Plan](#) details how relevant legislation and policies affect the way we handle personal information, the types of personal information held and the privacy complaint process. Employees should also read the [Privacy Statement for Southern Cross University's Websites](#).

Collecting personal information

We collect your personal information directly from you during the recruitment and induction processes and throughout the course of your time working with the University. The University will only collect your personal information from other sources (such as government agencies, medical practitioners, training providers) with your consent or in accordance with the law.

The University collects personal information such as your name, date of birth, contact details, tax file number, work history and health and safety information to facilitate and support your employment. The University's Privacy Management Plan provides a more extensive list of the types of information collected.

Providing this information is voluntary but if you choose not to provide information requested, it may stop the University from facilitating your recruitment or supporting your ongoing working arrangements. If you opt to provide it to us, we also collect information about your race/ethnicity, and sexual orientation/gender identity.

Likewise, where you provide the University with personal information in the course of your work indirectly, such as through the use of workplace IT or email systems, such information may be retained by the University and used in connection to your employment or working arrangements.

Using or disclosing personal information

The University will only use or disclose your personal information:

- For the purpose it was collected;
- For a directly related purpose;
- Where you have consented to an alternative use; or
- Where required or permitted by law.

Using Information

When the University holds personal information collected to facilitate, or in connection with your employment or working relationship, the University will retain and use that personal information to support and facilitate your matters directly connected to the ongoing working relationship.

Examples of how the University may use personal information to support processes associated with your employment or working relationship with us, include (but are not limited to):

- Recruitment, selection and appointment.
- Verification of details for employment purposes such as qualifications, experience, health and background checks and work rights.
- Payroll and superannuation administration.
- Industrial disputes.
- Insurance purposes.
- Workplace health and safety, fitness for work and workers compensation matters.
- Work related travel.
- Staff appraisals, probation, and promotion.
- Managing and investigating performance, conduct, and disciplinary matters.
- Staff training and development.
- Benchmarking, reporting, analysis, quality assurance and planning purposes;
- Managing complaints or workplace investigations.
- Informing you about University news and events, activities, courses and opportunities that may be of interest to you as a staff member of the University.
- Providing employees and workers with opportunities to access third party services, that are related to your employment or work, including engaging external providers who operate subject to their own privacy statement who may have access to your personal information in order to verify your right to access these services in connection to of your employment or working relationship.

Disclosing information

The University may disclose your personal information to third parties if required to facilitate or manage your employment. This may include:

- To check eligibility and suitability for employment.
- To organise travel, insurance, training and development.
- To facilitate pay and expenses including disclosing information to the ATO and superannuation funds.
- To organise staff mail-outs.
- To manage requests for workplace adjustments or workers compensation claims and to ensure safety of employees as required under work health safety laws.
- To defend proceedings or claims made against the University including providing information to solicitors or to an insurance company or insurer or its agent.
- To review and investigate complaints and to manage disciplinary or misconduct matters which may also include reporting concerns to relevant persons/authorities.
- To meet Government Department compliance requirements (eg. ATO, Department of Education and Training).
- To conduct votes for industrial instruments.
- Where necessary to prevent or lessen a serious and imminent threat to a person's life or health.
- Or otherwise required or permitted by law, including disclosing personal information under a subpoena or other lawful direction.

In addition, aggregated data about employees, with personal identifiers removed, is routinely provided to the Australian Bureau of Statistics, the Workplace Gender Equity Agency, Australian Higher Education Industry Association and various local and international university ranking bodies.

Workplace Surveillance

In accordance with the *Workplace Surveillance Act 2005* (NSW) and other applicable legal obligations, the University conducts ongoing and continuous surveillance of its campuses, buildings, Information technology (Technology Resources) and electronic communications (Digital Communications).

- Camera surveillance of its campuses and buildings ensure the safety of employees, students and visitors and the protection of property and buildings. Cameras operate in an overt surveillance manner (not hidden) and will be clearly visible and signed in the areas in which monitoring occurs. Camera recordings will be maintained for a period of time to allow the opportunity for review should an incident require further investigation.
- The University's Information Technology Conditions of Use Policy applies to all users of Technology Resources and Digital Communications. The University creates and monitors logs of all activities undertaken on Technology Resources. Monitoring may include activities such as which internet servers have been accessed, time and date of access, and University emails.

The University issues employees and workers with an identity (swipe) card to regulate access to approved buildings, rooms or other facilities. When the card is used the University will record details of the access including the name of the person issued the card, location, date and time of the access. These records (access logs) will be maintained for a period of time.

From time to time, lectures or meetings may be recorded. When this occurs, you will be advised.

Access and correction

The [Privacy Management Plan](#) contains information about:

- your right to access personal information the University holds about you;
- how to have personal information held by the University corrected; and
- how to complain about how your personal information has been handled.

Privacy Officer

Privacy enquiries should be directed to the University's Privacy Officer using the contact details below.

Privacy Officer
Southern Cross University
PO Box 157
LISMORE NSW 2480

e: privacy@scu.edu.au