Southern Cross University

Privacy Management Plan

Version 3: March 2022

Contents

1. Introduction

1.1 Context

Southern Cross University (the University) is an Australian public university established and operating under the *Southern Cross University Act 1993*.

Through teaching and learning activities, research, community engagement, as well as the provision of health, wellbeing and other services, the University collects, holds, uses and discloses a range of personal and health information relating to students, prospective students, alumni, staff, health clinic patients and third parties. Examples of the types of personal information held by the University can be found at Appendix 2.

Section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) requires the University to implement a Privacy Management Plan (Plan) that explains how the University manages personal and health information in accordance with its legal obligations.

This Plan also explains who to contact if you have questions about personal information collected and stored by the University, how to access and amend your personal or health information and what to do if you believe that the University may have breached your privacy.

1.2 Scope

This Plan has been prepared in accordance with section 33 of the PPIP Act and applies to all personal and health information held by the University and its controlled entities.

The Plan will be reviewed every year.

1.3 Controlled entities

The University's controlled entities must manage personal and health information in accordance with this Plan. Controlled entities may also have obligations under the Australian Privacy Principles and other legislation.

If a complaint or request for internal review is received by the University about the conduct of a controlled entity, the University may conduct a review if necessary.

1.4 Privacy law

The University is principally governed by NSW privacy legislation:

- *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act); and
- *Health Records and Information Protection Act 2002* (NSW)(HRIP Act).

Where applicable, this Plan also considers the requirements of the *Privacy Act 1998* (Cth), the European Union *General Data Protection Regulation* (GDPR), and China's *Personal Information Protection Law* (PIPL).

The *Privacy Act 1988* applies to:

i. Personal information the University collects and holds regarding student assistance provided by the Commonwealth, special circumstances remissions applications and tax file numbers.
ii. Personal information collected by the University's controlled entities.

iii. Personal and health information collected and held by the Southern Cross University Health Clinics.

Some provisions of the GDPR or the PIPL may apply to the University if it recruits staff or students who are living in the European Union or in China. Please contact the Privacy and Information Access Officer at privacy@scu.edu.au for more information.

Appendix 3 – Related information contains information about privacy laws and other privacy resources.

1.5 Privacy principles

This Plan is based around 12 Information Protection Principles (IPPs) found in the PPIP Act and 15 Health Privacy Principles found in the HRIP Act.

The *Privacy Act 1988* (Cth) also contains 13 Australian Privacy Principles (APPs) which cover both personal and health information and are broadly consistent with the IPPs and HPPs.

There are exemptions to some of the privacy principles, and criminal offences may apply to people who use or disclose personal or health information held by the University without authority to do so.

1.6 Information not covered by this plan

The following is not considered personal information and is not covered by this Plan:

- Information about an individual who has been dead for more than 30 years.
- Information that is already publicly available through the University website or other publicly available sources.
- De-identified information, i.e. where an individual cannot be identified from the information or data. De-identified information will be treated as personal information if an individual may be re-identified by being linked to other information.
- Information which relates to the University rather than the individual, for example the names and contact details of University staff members acting as employees of the University.

1.7 Related documents

In addition to this Plan, the University has a Privacy Policy and Privacy Data Breach Response Process that explain the procedures for managing a suspected privacy data breach, including notifying people whose privacy may have been breached and determining whether a privacy breach is subject to mandatory notification.

1.8 Accessibility

This Plan will be made available to staff and members of the public on the Privacy and Personal Information page of the University's website.

2. Managing privacy

2.1 Collecting personal information

The following explains how the University collects personal information, whether directly, indirectly or through automated processes. The University aims to ensure that all collection processes are open and transparent by providing privacy notices, terms and conditions of use, or other methods to communicate with individuals.

The impact on people's privacy must be considered whenever the University implements or reviews activities that involve the collection of personal information. This includes the implementation of new systems and processes. Please contact the Privacy and Information Access Officer at privacy@scu.edu.au for information and assistance.

2.1.1 Purposes for which information may be collected (IPP 1; HPP1)

The University will only collect personal information:

- For a lawful purpose;
- That is directly related to one of our functions or activities; and
- Where it is reasonably necessary for us to have the information.

Examples include:

- Teaching and learning
- Research
- Staff management including recruitment, performance management, professional development, remuneration, complaints and grievances, disciplinary matters and health, safety and wellbeing
- Student management including enrolment, academic progression, assessment, complaints and grievances, disciplinary matters, conferral and graduation
- Health Clinic management including appointments, referrals, and patient records management
- Community engagement including with potential staff and students, alumni, donors, community groups, other educational establishments, industry and government
- Marketing courses and student recruitment
- Provision of other services
- Administrative functions including receipt and payment of monies and managing security and safety of property and individuals

The University will allow people to receive services from us anonymously, where it is both lawful and practical to do so.

The University will only identify people using unique identifiers where it is reasonably necessary for our functions to do so. For example, a student number is a unique personal identifier allocated to each student, which enables efficient and effective student management and allows the University to distinguish between students who have the same name.

2.1.2 Collecting information directly (IPP 2; HPP 3)

The University will only collect information directly from an individual unless the individual consents to collection from someone else, or collection from a third party is required or permitted by law.

In line with IPP 4 and HPP 2, the University must also ensure that the information it collects is relevant, accurate, complete, up-to-date and not excessive. This means that the University must take care not to ask for irrelevant information or to intrude on the personal affairs of individuals.

For example, where a student applies for special consideration for health reasons, they should only be asked to provide enough information to evidence the impact that their current state of health will have on their ability to complete an assessment. Collecting information about previous health conditions or other personal matters would be irrelevant and excessive.

2.1.3 Collecting information from third parties

Individuals can authorise the University to collect their personal information from others, for example:

- Universities Admission Centre (UAC) - applicants authorise the University to collect their information from UAC for the purpose of assessment for the offer of a course of study.
- Prospective students and job applicants are informed that the University will verify qualifications or other information related to previous study or work history. By pursuing their application, they are consenting to the University doing so.
- Clients of the University's Health Clinics may authorise the Clinic to seek health information from other medical practitioners.

2.1.4 Collecting information through automated processes

The University may also collect information through the following automated processes:

- Security cameras located across all University campuses.
- Video recordings used for teaching and assessment purposes, for example recorded lectures or moots, or for staff training and development purposes, as well as through recording meetings conducted via online platforms such as Zoom or Microsoft Teams.
- Capturing information about visits to the University website or intranet for security and quality improvement purposes.
- Logging users of the University WiFi service and information management systems to facilitate the services.
- Logging staff and student access to University facilities such as offices and lecture rooms using swipe cards.

2.1.5 Privacy notices (IPP 3 and 6; HPP 4)

<u>When and how to provide a privacy notice</u>

An appropriate privacy notice must be provided whenever the University collects personal information. This includes information being collected verbally or by automated processes. Privacy notices help individuals to understand what personal information is being collected

and held by the University, the main purpose for which it is being collected and their rights to access and amend the information.

A privacy notice must be provided before information is collected or, if this is not possible, as soon as possible after the information has been collected. It is not appropriate to cover all University activities using one whole-of-University privacy notice.

A privacy notice may be provided:

- On a form that collects personal information or seeks consent
- On a web page
- In terms and conditions for an app or information system
- In a policy or procedure document

The privacy notice should be easily accessible to the individual concerned and be clearly distinguishable from any other information or instructions being provided.

Content

A privacy notice must include the following information:

- A statement that the University is collecting personal information, and what information is being collected.
- Why the information is being collected and how it will be used.
- Whether the information will be disclosed and, if so, to whom and for what reason.
- How an individual can access their information to amend or update it.
- Whether providing the information is voluntary or is required by law and whether there are any consequences for the individual if the information is not provided (or if consent to collect or hold the information is later withdrawn).

In some circumstances, it may also be necessary to inform individuals:

- If their information will be disclosed or transferred outside NSW or to a Commonwealth agency; and
- How consent can be withdrawn, for example the ability to unsubscribe from future marketing communications.

A sample privacy notice is provided on the University's Privacy and Personal Information webpage. Please contact the Privacy and Information Access Officer at privacy@scu.edu.au if you need help with customising a privacy notice

2.2 Security of personal information

2.2.1 Storage (IPP 5; HPP 5)

The University stores personal information securely, keeps it for no longer than is necessary and disposes of it appropriately. In addition, the University also takes reasonable steps to protect personal and health information from unauthorised access, use, modification or disclosure. This applies equally to computer/online storage and to paper-based storage systems.

Personal information is protected through a combination of security measures and practices including:

- University-wide policies and procedures. Relevant internal policies and procedures are identified in Appendix 3.
- Policies and procedures relating to access, use and disclosure of information developed by individual work units within the University, for example the University's Health Clinics.
- Corporate records management systems, which govern the capture, access, storage, retention and destruction of records in line with the University's obligations under the *State Records Act 1998* (NSW).
- Protection of information systems and data through passwords, security testing and monitoring and implementation of user rights and access controls.
- Enforceable contracts with third-party providers that host University systems or collect, store and process information on behalf of the University.
- Staff education and training.
- Privacy impact assessments.

2.2.2 Destruction

University records, including those containing personal information, are destroyed in accordance with the provisions of the State Records Act 1998 and related General Retention and Disposal Authorities.

The University provides secure destruction bins for the destruction of confidential documents, in line with the provisions of the Records Management Policy and Procedures. Work units that deal with highly sensitive information are also provided with document shredders.

Requests for destruction/erasure

Under the GDPR and the PIPL, some individuals have the right to request erasure or deletion, of their personal information.

In the event that an eligible individual makes such a request, the information will only be destroyed in line with the University's obligations under the *State Records Act 1998* (NSW) and any other applicable legislation.

2.2.3 Disclosing, transferring or storing personal information outside the University (IPP5 and 12; HPP 4 and 14)

The University may, at times, need to disclose, transfer or store personal information outside of the University.

If this is because the individual concerned has asked us to do so, any action taken by the University will be based on that individual's consent, for example, transferring their information to another university or health service provider.

The University uses information systems hosted by third parties and also uses cloud-based data storage systems. When engaging third parties, reasonable steps are taken to ensure that information being disclosed, transferred or stored externally remains secure, including through security testing and through privacy obligations in enforceable contracts.

Some University activities require information to be transferred or disclosed outside the NSW jurisdiction, or to Commonwealth agencies. Where possible, the University will seek the consent of the individuals concerned.

Exemptions may also apply to disclosing or transferring data outside NSW under the *Privacy Act 1998* (Cth), the GDPR or the PIPL.

2.3 Access

2.3.1 Access to personal information (IPP 6 and 7; HPP 7)

We will allow individuals to access their personal information without excessive delay or expense. In the first instance, individuals seeking access to their own personal information, or seeking information about whether the University holds their personal information, should email privacy@scu.edu.au, outlining what information they want to access and providing their contact details and proof of identity. In most cases access can be provided through an informal information request process and at no cost to the individual. Exceptions include:

- Where information is available for purchase, for example transcripts, testamurs or statements of course completion.
- Access is requested to health information.[1]
- Access is requested under the *Government Information (Public Access) Act 2009 (NSW)* (GIPA Act).

There may also be a cost if copies of documents are required.

Information about how to respond to requests for information from third parties and how to access government information under the GIPA Act can be found on the University website.

2.3.2 Amending personal information (IPP 8; HPP 8)

Individuals can update, correct or amend their personal information where necessary.

- Students can access and update their personal information, such as contact information, through My Enrolment or by contacting Student Administration Services – enquiry@scu.edu.au or call 1800 005 687.
- Staff can access and update their personal information through MyHR or by contacting HR Services – hr@scu.edu.au or call (02) 6620 3667.
- Patients of the University Health Clinics and Counselling Service can contact those services directly.

Please note that some changes, for example a change of name, may require supporting information. In accordance with IPP 8, if the University is not prepared to amend personal information as requested, reasonable steps will be taken to attach to the information a statement of the amendment that was sought.

[1] Requests for access to Health Clinic records must be made in writing addressed to either the relevant practitioner or the Health Clinic. Contact clinic@scu.edu.au for more information on accessing health records.

2.3.3 Refusing to provide access to information

In some circumstances, a request to access information may be refused. These include:

- Where the information is already available, either free of charge, for example through the University website, or for purchase through standard business processes, such as a replacement testamur.
- Providing access will disclose another person's personal information. Attempts will be made to remove the other person's information before the request is refused.
- The information is subject to legal professional privilege.
- It is believed that providing the information would pose a serious threat to the life or health of any individual.
- Refusal is required or permitted by law.
- Access would have a negative effect on law enforcement activities, or would prejudice a pending investigation or dispute resolution process.

Where access is refused, the following information will be provided to the individual in writing:

- The decision to refuse access with reasons why the decision was made; and
- How the decision can be appealed.

2.4 Using personal information (IPP 10; HPP 10)

2.4.1 General use

The University only uses personal information:

- For the purposes for which it was collected. This includes both the primary purpose and any secondary purposes identified in the privacy notice at the point of collection or
- For a directly related purpose or
- Where the individual concerned has provided consent or
- Where required or permitted by law or
- In the event of an emergency situation (see section 2.5.4 below).

The University may also use information for administrative purposes such as:

- Internal quality assurance and planning purposes. Information used for these purposes will be de-identified where it is possible and practical to do so.
- Handling complaints, investigations, appeals processes or litigation.

If a new use is identified for personal information that has been collected in the past, consent must be obtained unless the proposed new use is covered elsewhere in this Plan or is covered by a relevant exemption under privacy legislation. Please contact the Privacy and Information Access Officer at privacy@scu.edu.au regarding any potential new uses for information held by the University.

2.4.2 Withdrawal of consent

Where an individual withdraws consent for their information to be used, the University will take reasonable steps to comply with the request as soon as practically possible. Action to be

taken will depend on the context and nature of the request and will be in line with the University's responsibilities under *State Records Act 1998* (NSW) and any other applicable legislation.

2.4.3 Accuracy (IPP 9; HPP 9)

The University takes reasonable steps to ensure that personal information it collects and holds is relevant, accurate, up-to-date and complete before using it, including:

- Enabling staff and students to access and update their personal information through available IT systems.
- Providing regular email reminders to staff and students to keep their personal information up-to-date.
- Checking with callers to Student Administration Services that their personal information remains relevant, accurate and up-to-date.

Where practical, multiple sources of information will be limited in favour of having one, authoritative source of information that can be easily maintained and updated.

2.4.4 Research

Where personal information is collected or otherwise obtained for the purpose of undertaking research, this will be done in line with Human Research Ethics approval processes.

Privacy requirements and public interest considerations will be considered when approving research that requires collection and use of personal information.

Where research is in the public interest and cannot meet relevant privacy principles under the privacy acts, the research will be covered by the following statutory guidelines issued by the NSW Privacy Commissioner:

- Research involving personal information is covered by the Statutory Guidelines on Research – section 27B, Privacy and Personal Information Protection Act 1998 (NSW)
- Research involving health information is covered by the Statutory Guidelines on Research, Health Records and Information Privacy Act 2002 (NSW)

For more information contact ethics.lismore@scu.edu.au

2.4.5 Surveillance

Surveillance information relating to staff will be used in accordance with the *Workplace Surveillance Act 2005* (NSW). Activities that may generate surveillance information include:

- Security surveillance through CCTV footage undertaken for the protection of people and property. See the Closed Circuit Television (CCTV) Policy for more information. Signs are posted at various points on University campuses identifying CCTV cameras in use.
- Access to the University's physical locations via security passes.

Surveillance information may be used as evidence in internal investigations. Surveillance information may also be provided to an external third party in response to a lawful request.

Other activities that may generate surveillance information include:

- Monitoring access to and appropriate use of information systems and networks, in line with the University's Code of Conduct and Information Technology Conditions of Use Policy.
- Recording mileage and destination in log books when staff use University-owned vehicles.

2.4.6 Quality improvement and planning

The University uses information to improve the quality of its services, functions and activities. This primarily involves the use of statistical information, but may also include the use of personal information. If personal information is to be used in this way, it will be referenced in privacy notices at the point of collection.

2.5 Disclosing personal information (IPP 11 and 12; HPP 12)

2.5.1 When personal information may be disclosed

Personal information may only be disclosed:

- For the purposes for which it was collected. This includes both the primary purpose and any secondary purposes identified in the privacy notice at the point of collection; or
- Where the individual has provided consent, or where the individual would be aware that such a disclosure will occur; or
- For a directly related purpose and where there is no reason to believe that the individual concerned would object to the disclosure; or
- Where disclosure is necessary in an emergency situation (see section 2.5.4 below).

The University cannot disclose sensitive personal information (defined in Appendix 1) without a person's consent, unless the disclosure is necessary in order to deal with a serious and imminent threat to any person's health or safety.

Examples of when information may be disclosed include, but are not limited to:

- Where an external company is contracted to host or provide support for a business system that holds personal information.
- Verification of the authenticity of academic records or qualifications.
- Management of investigations, appeals or complaints processes, or disclosure in relation to insurance matters or litigation.

There are also exemptions to these limits on the disclosure of personal information, such as when disclosure is permitted by law, for example:

- Where legislation requires that information must be disclosed to government agencies such as the Australian Taxation Office (ATO), federal education or immigration departments or Centrelink, or for mandatory reporting requirements under the *Health Practitioner Regulation National Law*. Routine disclosure of information under legislation should be included in the relevant privacy notice.
- Where information is requested by a valid subpoena, warrant or court order.

- Where disclosure is required for legitimate law enforcement purposes and is covered by exemptions under privacy legislation.

The University does not have any Memorandums of Understanding or referral arrangements with other agencies relating to the sharing of disclosure of personal information.

Requests for information under subpoena, warrant or court order, or for law enforcement purposes, should be directed to The Proper Officer, University Legal Office by email to legal@scu.edu.au or call (02) 6620 3465.

If information has been disclosed beyond its primary purpose (or any related purposes, where consent has been provided or where any exemptions have been used) details of the decision to disclose and the process involved must be approved by the relevant Executive member or Head of Work Unit and the decision be documented and retained in accordance with the Records Management Policy and related Procedure.

2.5.2 Internal access to personal information

In general, providing information to different work units within the University is not considered disclosure. However, personal information should only be accessed by or, provided to, staff members who require the information for a legitimate use. In particular, access to health information is tightly controlled and generally limited only to University work units that are involved in processing health information, such as the Health Clinics, or HR Services.

Professional staff in areas such as the Legal Office, Technology Services and Corporate Records may have access to files and documents that contain personal information. All University staff are governed by the University Code of Conduct and relevant policies and procedures governing appropriate access and use of information.

Information may also be provided to relevant University staff where it is necessary for:

- Handling complaints
- Management of potential or actual litigation
- Internal audit and investigations
- Reviews or investigations into alleged breaches of policy, rules or legislation

2.5.3 Additional requirements covering use or disclosure of health information (HPP 10 and 11)

The University may disclose health information where it is considered necessary for:

- the management of health services
- training purposes, subject to informed consent, or
- research which is approved by the Human Research Ethics Committee (see section 2.4.4 above)

The NSW Privacy Commissioner can provide further information and a range of privacy resources for NSW Health Service Providers.

In line with HPP15, the University will not link an individual's health record with those of another organisation without the individual's express written consent.

2.5.4 Use or disclosure of information in emergency situations

Personal information may be used or disclosed in an emergency situation, as defined in the *State Emergency and Rescue Management Act 1989*, s4, or where it is considered necessary to lessen or prevent an imminent and serious threat to the life or health of an individual. With regard to health information, this includes a serious threat to public health and safety.

Approval for the immediate use or disclosure of information in emergency situations must be obtained from one of the following staff members, as appropriate in the circumstances:

- Vice Chancellor or Vice President (Operations)
- Director, Student Administration Services, or Deputy Vice Chancellor (Students) in relation to information about current, past or prospective students.
- Director, Human Services in relation to information about current, past or prospective staff members, contractors or volunteers.
- A registered medical practitioner in relation to a patient's information.
- Relevant member of the Executive in relation to information that falls within their portfolio.
- Manager, Security Services where information is required to be released to police after hours, and where approval from any of the above is unavailable.

The approval must be documented and retained in accordance with the Records Management Policy and related Procedure.

2.5.5 Third parties acting on behalf of an individual

Unless permitted under the privacy acts and any applicable exemptions, consent must be obtained before the University will communicate with a third party on an individual's behalf in relation to their personal information or personal affairs.

Where an individual is unable to provide consent, or is incapable of doing so, the University may liaise with a third party under a power of attorney or a nominated emergency contact in a limited capacity, for example:

- By assisting with special consideration applications.
- Staff leave arrangements where an individual is in hospital and is unable to liaise with the University themselves.

Deceased individuals

For deceased individuals, the authority to provide consent or otherwise liaise with the University lies with the deceased person's executor or next of kin.

Minors

The University may collect personal information about a minor (a person aged under 16 years) from a parent or legal guardian. Where it is considered to be in the best interests of a minor, the University may also disclose personal information to a parent or legal guardian. However, the maturity of the minor and the context should be taken into consideration before liaising with a parent or guardian. In some situations, it may be a breach of a minor's privacy to liaise with their parents or legal guardian.

Details of the decision to disclose information to a parent or legal guardian, and the process involved must be approved by the relevant Executive member or Head of Work Unit and the decision be documented and retained in accordance with the Records Management Policy and related Procedure.

In relation to health information, consultation with a parent or legal guardian will be determined on a case-by-case basis and will depend on the nature of the medical issues concerned and the maturity of the individual. This will be a decision for the medical practitioner concerned in consultation with the Health Clinic Manager.

2.6 Exemptions to privacy requirements

2.6.1 Exemptions under legislation

As noted elsewhere in this plan, there are exemptions to the IPPs and HPPs in the NSW privacy acts.

The University may also be exempt from complying with the privacy principles where action is required or permitted under another law.

The University will only rely on exemptions to the privacy principles where it is appropriate to do so under the circumstances. Please contact the Privacy and Information Access Officer at privacy@scu.edu.au if you are considering relying on an exemption.

2.6.2 Public interest directions

The NSW Privacy Commissioner may make public interest directions that modify the application of privacy principles in some circumstances.

The University will only apply public interest directions that are applicable in the circumstances.

2.6.3 Public registers

The University does not hold any formal public registers containing personal information under the NSW privacy acts.

2.7 Assessing privacy impacts

Staff should consider the requirements of the IPPs and HPPs when implementing or reviewing projects, processes and systems. Where a proposed activity or change to an existing activity is likely to affect an individual's privacy or involve the collection, storage, use or disclosure of personal information, a privacy impact assessment is recommended. This includes the development and implementation of information systems.

An assessment tool is available to assist staff to undertake the assessment process.

The Australian Privacy Principles (APPs) should also be considered if an activity is governed by federal legislation that requires compliance with the APPs.

Consultation with different areas of the University, for example Legal Office, Technology Services, Governance Services or the Privacy and Information Access Officer, is recommended at various stages of the assessment process to ensure that the correct advice is received and that all relevant information has been considered. For example, where the activity involves

using third party software or an externally hosted IT system, Technology Services must be consulted.

2.8 Privacy data breach reporting

Although processes are in place to protect personal information, if information is lost or subject to unauthorised access, modification or disclosure, a privacy data breach will have occurred and must be managed in accordance with the University's Privacy Data Breach Response Process.

3. Education and support

3.1 Policy and governance

The Privacy Policy sets out the University's privacy requirements and is supported by this Plan. Privacy requirements may be incorporated into other governance and policy documents and will be cross-referenced where appropriate.

3.2 University procedures and guidance

Privacy-related procedures can be accessed through the University policy library.

Information about privacy-related matters can be found on the University website.

3.3 Staff orientation and induction

All University staff have obligations and responsibilities under NSW privacy legislation.

Supervisors are responsible for ensuring that staff under their supervision, including contractors and casual staff are informed of their privacy responsibilities and provided with information about privacy resources, as part of their staff orientation. This may include general privacy training, as well as local induction into information management and privacy matters specific to the work unit.

3.4 Privacy training

Heads of Work Unit are responsible for ensuring that staff undertaking business processes or accessing information systems understand the specific privacy requirements regarding the appropriate collection, storage, use and disclosure of personal or health information in their work area.

Online Privacy Awareness Training is available to all staff through the HR PLP Professional Learning Centre, which is accessed through My SCU. Customised training can also be arranged for work units that deal with personal information on a regular basis.

Please contact the Privacy and Information Access Officer at privacy@scu.edu.au for more information.

4. Communication with individuals

The University primarily communicates with individuals through the use of privacy notices and consent forms at various points where personal information is collected (see section 2.1.5 of this plan). Other privacy-related communications include:

- How an individual can access or correct their personal information (see section 2.3.2 of this plan).
- Responding to requests for information from third parties (information can be found on the University website).
- Identity verification (see section 4.1 below).
- Surveillance activities (see section 2.4.5 of this plan).
- How an individual can make a privacy complaint (see section 5 of this plan).

4.1 Identity verification

Before dealing with an individual about their personal information, the University will require the individual to confirm their identity. This also applies to any third parties that have authority to act on an individual's behalf. This is to ensure that the University does not breach an individual's privacy by providing their personal information to the wrong person.

Identity may be verified by one or more of the following:

- Staff or student ID number and date of birth.
- Use of student, alumni or staff email accounts. Emails received from these accounts are considered to be from the individual concerned without the need for additional identification. Communication that is received from any non-University email account will require verification of identity.
- Photo identification such as current staff or student card, valid passport or drivers' licence. Where enquiries are made in person, sighting of the ID may be sufficient. Enquiries made in writing, by email or by telephone may require a copy of identification documents to be provided.

5. Complaints

5.1 Making a complaint

If an individual believes that the University has breached their privacy, they should contact the work unit responsible as soon as possible. In most cases, these matters can be dealt with quickly and informally by the work unit concerned.

Privacy complaints that relate to research activities, such as the handling of research data, will be initially referred to the Office of the Deputy Vice Chancellor (Research).

If an individual is not satisfied with the response of the work unit, they may make a formal complaint about a breach of privacy by contacting the Privacy and Information Access Officer at privacy@scu.edu.au. Formal complaints will be dealt with through a privacy internal review.

An individual may also complain directly to the NSW Privacy Commissioner.

5.2 Privacy internal review

Any privacy complaint that meets the criteria for internal review under the PPIP Act, will be dealt with as such, regardless of whether the complainant specifically requests an internal review.

5.2.1 Application

An application for internal review must:

- Be made in writing to the University. You may use the Information and Privacy Commission Internal Review Application Form.
- Include an Australian address for correspondence;
- Be lodged with the University within six months of the complainant first becoming aware of the conduct that is being complained about; and
- Provide sufficient information for the complaint to be investigated.

5.2.2 Internal review process

When the University receives an internal review application, the Privacy and Information Access Officer will:

- Send an acknowledgment letter to the applicant and advise that, if the internal review is not completed within 60 days, they have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal (NCAT); and
- Send a letter to the NSW Privacy Commissioner, together with details of the application and a copy of the written complaint.

Internal reviews follow the process set out in the New South Wales Information and Privacy Commission ("IPC") Internal Review Checklist.

The University is required to check whether the Privacy Commissioner wishes to make a submission in relation to an internal review. The University will do this by sending a draft copy of its preliminary determination to the IPC. The University must consider any submission made by the Privacy Commissioner with respect to an internal review.

5.2.3 Internal review outcomes

An internal review must be completed within 60 days of receipt of a valid application, unless an extension of time is negotiated with the applicant. When the internal review is completed, and the University has received a response from the Privacy Commissioner about our draft preliminary determination, the University will notify the applicant in writing of:

a. The findings of the review;
b. The reasons for the finding, described in terms of the IPPs, HPPs or APPs;
c. Any action it proposes to take;
d. The reasons for the proposed action (or no action); and
e. The applicant's entitlement to have the findings and the reasons for the findings reviewed by the NCAT.

A copy of this letter will also be sent to the Privacy Commissioner.

Statistical information about the number of internal reviews conducted must be provided in the University's Annual Report.

5.3 External reviews and appeal rights

If an applicant is not satisfied with the outcome of handling an internal review, they can apply for external review of the decision by the NCAT.

The application must be made within 28 calendar days of receiving notice of an internal review decision.

Where an internal review is not completed within 60 days, the 28 calendar day time limit starts when the 60 day period has expired.

Please see the NCAT website for more information on the external review process.

5.4 Policy breaches and misconduct

Breaches of this Plan will be managed in line with relevant policies and procedures, including the Privacy Data Breach Response Process, Code of Conduct, and Rules – Student Academic and Non-Academic Misconduct Rules.

Individuals who deliberately breach privacy legislation may be held personally liable for that action and attract legal penalties under the PPIP Act or HRIP Act or criminal prosecution under the *Crimes Act 1900* (NSW). The following offences can be found in Part 8 of the PPIP Act:

- intentionally disclose or use personal information accessed as part of your work for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully and
- hinder the Privacy Commissioner or a staff member from doing their job.

Third parties may be also be personally liable if they attempt to bribe or engage in forms of corrupt behaviour to induce a staff member to breach privacy principles.

6. Privacy contacts

6.1 Internal contacts

Initial enquiries about privacy matters should be directed to the work unit that holds the information.

Prospective, current and former students who want to enquire about information the University holds about them should contact Student Administration Services in the first instance.

Prospective, current and former staff can enquire about information held centrally by contacting HR Services in the first instance.

Other enquiries should be directed to the Privacy and Information Access Officer at privacy@scu.edu.au.

6.2 External contacts

NSW Privacy Commissioner
Information and Privacy Commission (IPC)
GPO Box 7011, Sydney, NSW 2001
Telephone: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NSW Civil and Administrative Tribunal (NCAT)
Telephone: 1300 006 228
Website: www.ncat.nsw.gov.au

Appendix 1
Definitions

Collection is how the University acquires personal or health information. Collection can be by any means, for example a written or online form, a verbal or online conversation, a voice recording, photography or video recording.

Disclosure means when we provide personal information to an individual or organisation outside the University.

Health information is information or an opinion about:

i. a person's physical or mental health or disability;
ii. a person's express wishes about the future provision of their health services; or
iii. a health service provided, or to be provided, to a person.

See the full definition at section 6 of the HRIP Act.

Investigative agency means any of the following - the Ombudsman's office, the Independent Commission against Corruption (ICAC) or the ICAC Inspector, the Law Enforcement Conduct Commission (LECC) or the LECC Inspector or any staff of the Inspector, the Health Care Complaints Commission, the Office of the Legal Services Commissioner, the Ageing and Disability Commissioner. It also includes a person or body prescribed by regulations. In respect of personal information, it may also include other public sector agencies with investigative functions. See the full definition at section 3 of the PPIP Act

Law enforcement agency means any of the following:

i. In relation to personal information - the NSW Police Force or the police force of any other State or Territory, the NSW Crime Commission, the Australian Federal Police, The Australian Crime Commission, The Director of Public Prosecution of NSW or of another State or Territory or the Commonwealth, the Department of Justice, the Office of the Sherriff of NSW.
ii. In relation to health information - - the NSW Police Force or the police force of any other State or Territory, the NSW Crime Commission, the Australian Federal Police, The Australian Crime Commission, The Director of Public Prosecution of NSW or of another State or Territory or the Commonwealth, the Department of Corrective Services, the Department of Juvenile Justice.
iii. It also includes a person or body prescribed by regulations.

Personal information is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes information or an opinion recorded in a database, and also information or an opinion that that is not recorded in a material form. There are also a number of exclusions from the definition of personal information.

See the full definition at section 4 of the PPIP Act, including the exclusions at section 4(3).

Primary purpose means the main reason for which personal information has been collected. An example would be collecting personal information for the purpose of student enrolment.

Privacy Acts generally means *the Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and *Health Records and Information Protection Act 2002* (NSW)(HRIP Act). Where applicable, *Privacy Acts* may include the *Privacy Act 1998* (Cth), the European Union *General Data Protection Regulation* (GDPR) and China's Personal Information Protection Law.

Privacy notice means a notice or statement which explains what personal information is being collected, the purpose of collection, how the information will be used, whether it will be disclosed and, if so, to whom, and how it can be accessed.

Privacy obligations means the privacy principles (see section 1), specific obligations under this plan and any exemptions to those principles that apply to the University.

Privacy principles are the Information Protection Principles (IPPs) set out in Division 1 of Part 2 of the PIPP Act and the Health Privacy Principles (HPPs) set out in Schedule 1 of the HRIP Act. These set out the minimum standards for all NSW public sector agencies when handling personal and health information, unless an exemption applies.

Secondary purpose means any purpose for which information is collected, other than the primary purpose, that is identified in a privacy notice. An example would be to provide information about scholarships or prizes, where the primary purpose for collection is for student enrolment.

Sensitive personal information means information about a person's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or union, or sexual preferences or practices.

Appendix 2
Types of information collected and held

Below is an overview of the types of personal or health information collected and held by the University in relation to its functions, outlined in section 1.1 of this Plan.

Teaching and learning

- Assessments and coursework completed by students;
- Comments and personal details provided through feedback and survey responses.

Research

- Personal information collected through research projects;
- Personal information of researchers applying for research or grant funding.

Managing staff (including recruitment, performance, remuneration, safety and wellbeing)

- Staff details, including but not limited to, date of birth, contact details, emergency contact details, tax file declarations, banking details, contracts of employment, previous work history, salary details, superannuation information, leave applications and approvals (including medical certificates where relevant), EEO information, training history, eligibility to work in Australia;
- Recruitment information (for both successful and unsuccessful applicants) including contact details, applications, CVs, previous work history, referee reports, skills assessments, police and working with children checks where applicable;
- Health and safety-related information, including workers compensation claims, and details of accidents and injuries, including relevant health information provided;
- Information relating to grievance, complaint and misconduct processes and any subsequent appeals;
- Performance planning, including work plans, probation plans, reports and performance reviews.

Managing students (including enrolment, assessment and graduation)

- Student details, including but not limited to, photograph, date of birth, contact details, emergency contact details, previous education, subjects/courses studied, qualifications attained, fee payments, banking details, fines and debt information if applicable, ethnicity, indigenous status, language, visa and immigration status, exchange details and sponsorship details where relevant;
- Information relating to applications for enrolment, leave, special consideration, withdrawals etc, including health or personal information provided to support those applications;
- Assessment and examination records, including marks, comments and final grades;
- Supervision records including progress reports, attendance records etc;
- Information relating to grievance, complaint and misconduct processes and any subsequent appeals;
- Course, subject and timetable information where this is linked to identifiable individuals;

- Details of internships, placements, fieldwork and other forms of professional experience, including results, evaluation and where applicable, criminal history checks, vaccination records and working with children checks;
- Information about graduands including names, contact details, faculty, course and qualification;
- Applications for and receipt of, prizes, awards and scholarships;
- Details of disabilities, Overseas Student Health Cover details and medical history where relevant.

Community engagement (including potential staff, students, donors, community groups, other educational institutions, industry and government)

- Alumni names and contact details;
- Personal and health information for students attending short courses and summer school programs;
- Donor information including names, contact details, history of engagement with the University, dates, amounts, conditions of any gifts or bequests;
- Names and contact details of prospective students;
- Names and professional contact information for career advisors, principals, teachers, industry partners and professional bodies;
- Attendee information for events, short courses and functions including names, contact details, position titles, organisation details, dietary requirements.

Providing services to staff and students

- Medical records, including personal information and confidential health information collected in the course of providing health services through the Southern Cross University Health Clinics or the Student Counselling Service;
- Personal information relevant to requests for services such as parking permits, career support, disability support, assistance with grievances, financial assistance, study support, support for Aboriginal and Torres Strait Islander students, renting of student accommodation;
- Information related to library use including contact information, photo ID, borrowing record, fines etc.

Administrative functions (including receipt and payment of monies, security and safety of property and individuals).

- Financial details, such as bank account details;
- Security incident reports and information captured by CCTV;
- Access logs and audit trails of staff and student activity in relation to use of IT systems;
- Personal and health information captured through work health and safety reports;
- Personal details of nominated, appointed and elected committee members;
- Personal information of people making applications for access to information under the GIPA Act; and
- Personal information relevant to processing warrants, subpoenas, court orders, contracts and other legal matters.

Appendix 3
Related information

1. University policies and governance documents

Closed Circuit Television (CCTV) Policy
Code of Conduct
Information Technology Conditions of Use Policy
Rules – Student Academic and Non-Academic Misconduct Rules
Privacy Data Breach Response Process
Privacy Policy
Records Management Policy
Records Management Procedure

2. Other internal privacy resources

Privacy and Personal Information webpage

3. External resources

Legislation

Personal Information Privacy Law 2021 (People's Republic of China)
European Union General Data Protection Regulation 2017
Government Information (Public Access) Act 2009 (NSW)
Health Records and Information Privacy Act 2002 (NSW)
Privacy Act 1998 (Cth)
Privacy and Personal Information Protection Act 1998 (NSW)
Southern Cross University Act 1993 (NSW)
State Records Act 1998 (NSW)
Workplace Surveillance Act 2005 (NSW)

Other resources

Checklist – Identifying privacy issues
Checklist – Privacy for NSW Public Agencies
Consent – use or disclosure of personal or health information
General Retention and Disposal Authorities (State Archives and Records Authority NSW)
Statutory guidelines on the management of health services (HRIP Act)
Statutory Guidelines on Research (HRIP Act)
Statutory Guidelines on Research – section 27B (PPIP Act)
Statutory guidelines on training (HRIP Act)