Privacy Management Plan

Section 1 - Purpose and Scope

Purpose

(1) The purpose of this Privacy Management Plan (Plan) is two-fold:

a. it demonstrates to members of the public how Southern Cross University upholds and respects the privacy of the students, staff and others about whom we hold personal information; and
b. it acts as a reference tool for University staff, to explain how we may best meet our privacy obligations under the Privacy and Personal Information Protection Act 1998 (NSW), the Health Records and Information Privacy Act 2002 (NSW) and the Privacy Act 1988 (Cth).

Scope

(2) This Plan applies to all personal information and health information (including sensitive information) held by the University and its controlled entities.

(3) The Plan has the status of Policy for the purposes of the Governance Documents Rule.

(4) This Plan has been prepared in accordance with Section 33 of the Privacy and Personal Information Protection Act 1998 (NSW).

Section 2 - Definitions

(5) "Collection" (of personal information)

a. means the way the University acquires the information. Collection can be by any means. Examples include: a written form, a verbal conversation, an online form, or taking a picture with a camera.

(6) "Disclosure"

a. means when we provide personal information to an individual or body outside the University - or, in some cases, to other discrete units within the University.

(7) "Health information"

a. means personal information that is also information or an opinion about:
    i. a person's physical or mental health or disability;
    ii. a health service provided, or to be provided, to a person;
    iii. a person's express wishes about the future provision of health services to him or her;
    iv. other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue; or
    v. genetic information that is or could be predictive of the health of a person or their relatives or

descendants.

(8) "Holding" personal information

a. the University will be considered to be 'holding' personal information if it is in the University's possession or control, or if it is held by a contractor or service provider on our behalf. Most of the privacy principles apply to when the University is 'holding' personal information, which means we remain responsible for what our contractors or service providers do on our behalf.

(9) "HRIP Act"

a. means the Health Records and Information Privacy Act 2001 (NSW).

(10) "Personal information"

a. means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
    i. Personal information can include information that is recorded (e.g. on paper or in a database), but also information that is not recorded (e.g. verbal conversations). It can even include physical things like a person's fingerprints, tissue samples or DNA.
    ii. Some things are exempt from the definition of "personal information", including information about a person who has been dead for more than 30 years, and information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
    iii. Also note that "health information" is sometimes treated a little differently to other types of "personal information", and has its own definition - see above. There are also some special rules for "sensitive personal information" - see below.

(11) "PPIP Act"

a. means the Privacy and Personal Information Protection Act 1998 (NSW).

(12) "Privacy obligations"

a. means the privacy principles, specific obligations under Section 5 - of this Privacy Management Plan and any exemptions to those principles that apply to the University.

(13) "Sensitive personal information"

a. 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.

(14) "University"

a. means Southern Cross University and its controlled entities.

(15) "Use"

a. means when the University uses personal information for some purpose.

Section 3 - Southern Cross University and its Privacy Context

(16) The University is an Australian public university established and operating under the Southern Cross University Act 1993 (NSW). The University holds a vast amount of personal information not only pertaining to the students we serve, but also relating to our staff. The University will protect privacy with the use of this Plan as a reference tool.

(17) As a NSW public sector agency, the University is primarily regulated by the PPIP Act and the HRIP Act. Additionally, the Privacy Act 1988 (Cth) applies to:

a. personal information the University collects and holds regarding student assistance provided by the Commonwealth, special circumstances remissions applications, and tax file numbers; and
b. to all personal information collected by the University's controlled entities.

(18) Each of PPIP Act, HRIP Act and Privacy Act 1998 (Cth) centres around what are termed 'privacy principles'. The PPIP Act covers personal information other than health information, and requires the University to comply with 12 information protection principles (IPPs). The IPPs cover the full 'life cycle' of information, from the point of collection through to the point of disposal. They include obligations with respect to data security, data quality (accuracy) and rights of access and amendment to one's own personal information, as well as how personal information may be collected, used and disclosed.

(19) Health information is regulated by a slightly different set of principles under the HRIP Act. Health information includes information about a person's disability, and health / disability services provided to them. There are 15 health privacy principles (HPPs) in the HRIP Act, with which the University must comply. Like the IPPs, the HPPs cover the entire information 'life cycle', but also include some additional principles with respect to anonymity, the use of unique identifiers, and the sharing of electronic health records.

(20) The Privacy Act 1988 (Cth) contains 13 Australian Privacy Principles (APP) which cover both personal and health information. The APPs are broadly consistent with the IPPs and HPPs prescribed under the PPIP Act and HRIP Act, however, with respect to receipting unsolicited information, cross border disclosures of information, and direct marketing, the APPs prescribe more stringent safeguards which the University applies to the handling of the information described at clause (17).

(21) There are exemptions to many of the privacy principles. There are also criminal offence provisions applicable to employees of the University who use or disclose personal information or health information without authority.

Types of personal and health information held

(22) Examples of personal information held by the University are:

a. Personnel and payroll records including:
    i. payroll and pay related records, including banking details;
    ii. tax file number declaration forms;
    iii. medical assessment records;
    iv. attendance and leave records;
    v. recruitment, appeals, promotion and transfer records;
    vi. personal employee files and service records;
    vii. counselling and discipline records;
    viii. performance management and evaluation records;

ix. training records;
x. notices of separation and exit questionnaires;
xi. occupational health and safety and workers compensation records;
xii. records of gender, ethnicity and disability of employees for equal employment opportunity reporting purposes;
xiii. recruitment applications, references and reports;
xiv. records relating to character checks and criminal convictions; and
xv. fitness to work statements.

b. Student records including:
   i. records of name, date of birth, home address and other personal information of students gathered as part of various application processes;
   ii. health information relating to students such as:
      - information about a student's disabilities and needs (where applicable);
      - records of counselling appointments made and attended by students as part of their interaction with the Health chapter of Student Services.

c. Records of patients of the University's Health Clinic, and of individuals associated with the clinical/professional placements of students across the University:
   i. records of name, date of birth, home address and other personal information of patients gathered as part of health assessment processes;
   ii. information about the health status and medical treatment of patients; and
   iii. special circumstances remissions applications which may contain health information.

Inventory of the University's Significant Information Systems

System	Purpose
Academic Integrity Database:	Excel-based database for registration and monitoring of current and past academic integrity issues.
Aurion	Human Resources information database (including some payroll capacity).
CONRAD:	(Continuity Register And Database) - clinical placements database used specifically for storage of information relating to midwifery projects.
Corporate Records System:	Corporate records keeping system.
CRM:	Customer Records Management (system) - customer relations database for logging and monitoring interaction with student and non-student enquiries.
E-learning / Blackboard learning system:	Student electronic interactive learning interface (host of podcasts, 'Illuminate' portal, etc.).
Email system:	Staff and student email system.
Etrans:	A purchasing and authorisation database utilised University-wide.
Filemaker Pro:	logging and storage electronic database utilised by Student Services.
Finance One:	The University's core finance system.
IRMA	A database used within the Division of Research for recording research publications, contracts and grants, higher degree research students and animal and human ethics records.
LEX	Records management system used with the University Legal Office.
MIS:	Management Information System
SONIA:	Clinical placements database.

Student One (Student Management System):	Student information database with differing levels of access, and two separate portals - one for students, and another for University staff.

Section 4 - Privacy Management Principles

Introduction

(23) The privacy principles are the standards which the University implements when dealing with personal information (including health information).

(24) The University's 'privacy principles' are based on a combination of the 12 IPPs (in Sections 8 to 19 of the PPIP Act) and the 15 HPPs (in Schedule 1 of the HRIP Act). The principles are consistent with most requirements of the APPs (in the Privacy Act 1988 (Cth)). However, to the extent the IPPs and HPPs do not fully meet the APP requirements, Section 5 - of this Plan provides additional principles for specific and limited use.

(25) There are a number of ways that our conduct may be exempt from one or more of the IPPs, HPPs or APPs. Exemptions are found in the Acts themselves, in temporary Directions made by the Privacy Commissioner, and in Privacy Codes of Practice. In some cases, other legislation will override the privacy principles. If in doubt, you should always check the exact wording in the legislation.

(26) The following section uses plain language (not the wording of the law itself) to describe the privacy principles and how University staff must comply with them. It also mentions the exemptions that may be relevant for the University, depending on the context.

(27) If you need guidance on interpreting the requirements of the privacy principles or exemptions, please contact the University's Privacy Contact Officer.

The Principles

(28) Our privacy obligations for all personal information and health information have been condensed into one set of 13 plain language principles to be followed by the University:

a. Limiting Our Collection of Personal Information;
b. Anonymity;
c. Unique Identifiers;
d. How We Collect Personal Information - the Source;
e. How We Collect Personal Information - the Method and Content;
f. Notification When Collecting Personal Information;
g. Security Safeguards;
h. Transparency;
i. Access;
j. Correction;
k. Accuracy;
l. Use; and
m. Disclosure.

(29) Specific and additional obligations which relate to the management of information subject to the Privacy Act 1988 (Cth) as listed at clause (17) are defined in Section 5 - of this Privacy Management Plan.

Part A - Limiting Our Collection of Personal Information

(30) We will only collect personal information if:

a. it is for a lawful purpose that is directly related to one of our functions, and
b. it is reasonably necessary for us to have the information.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

We won't ask for personal information unless we really need it. In particular, we will avoid collecting "sensitive information" if we don't need it.

By limiting our collection of personal information to only what we really need, it is much easier to comply with our other obligations.

Example: when designing a form, ask yourself: "do we really need each bit of this information?"

Example: If we need to know a person's age to provide age-appropriate services, we will ask for their age or year of birth, not their date of birth.

Common exemptions

Unsolicited information

Information collected before 1 July 2000

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Part B - Anonymity

(31) We will allow people to receive services from us anonymously, where lawful and practicable.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

Example: Potential 'customers' of the University should be provided with information about the University's programs and services, without having to identify themselves.

Common exemptions

None.

Part C - Unique Identifiers

(32) We will only identify people by using unique identifiers if it is reasonably necessary for our functions.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

Identifiers can assist with efficient record management, but they also pose privacy risks if they are used to match or compile large quantities of data about a person from different sources. For that reason, sharing unique personal identifiers between different organisations is generally prohibited.

A unique personal identifier is not just a person's name or file number. It can be a key (such as a number) which aims to uniquely identify a person - for example so that you can separate all the different people with the name 'John Smith'.

A student number, tax file number, a unique patient number or a driver's licence number is a unique personal identifier.

Common exemptions

None.

Part D - How We Collect Personal Information - the Source

(33) We will only collect personal information directly from the person unless they have authorised otherwise.

Special rule for health information or sensitive information?

Yes. The rule for health information is a little easier. We must collect health information directly from the person, unless it is unreasonable or impractical to do so.

Key messages, examples and definitions

If we need information about Sue, we should ask Sue herself, rather than Jim.

By collecting information direct from the source, it will be easier for us to comply with other obligations too, like ensuring the accuracy of the information, and getting permission for any disclosures of the information.

Example: A student has fainted and a representative from Student Services has called the first aid officer. It is OK to ask the student's friend for some health information about the student ("is the student diabetic?") because it is unreasonable and impractical to ask the student directly.

Example: Potential students have already authorised UAC to provide their information to the University on their behalf, when applying for a course at the University.

Common exemptions

Unsolicited information.

Where the person is under 16, we can instead collect the information from their parent or guardian (but we don't have to).

If another law authorises or requires us to collect the information indirectly (i.e. from a different source).

For some law enforcement and investigation purposes.

When we are taking a family, social or medical history from a client of our health or counselling services.

Information collected before 1 July 2000.

If compliance would, in the circumstances, prejudice the interests of the individual to whom the information relates.

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Other relevant points

Where a person lacks some capacity (e.g. because of a brain injury), we can ask their authorised representative for the information instead. But we must also still try to communicate with them directly. Privacy NSW's Best Practice Guide Privacy and people with decision-making disabilities explains how to collect personal information from or about a person who has limited or no capacity.

Privacy NSW's Handbook to Health Privacy provides some other examples of when it might be "unreasonable or impractical" to collect health information directly from the person.

Part E - How We Collect Personal Information - the Method and Content

(34) We will not collect personal information by unlawful means.

(35) We will not collect personal information that is intrusive or excessive.

(36) We will ensure that the personal information we collect is relevant, accurate, up-to-date, complete, and not misleading.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

We won't ask for information that is not relevant, very personal, or might become out of date. But we only need to take 'reasonable steps' to ensure we meet this standard.

To determine what might be 'reasonable steps', we will consider:

the sensitivity of the information;

the possible uses of the information; and

the practicality and cost of aiming for 'best practice'.

Example: PQR wants to do a student satisfaction survey or conduct teacher or unit feedback studies. It is not relevant for the University to know each student's or teacher's home address, date of birth or marital status.

Common exemptions

Unsolicited information

Information collected before 1 July 2000

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Part F - Notification When Collecting Personal Information

(37) When collecting personal information, we will take reasonable steps to tell the person:

a. our contact details;
b. who will hold and/or have access to their personal information;
c. what it will be used for;
d. what other organisations (if any) routinely receive this type of personal information from us;
e. whether the collection is required by law;
f. whether we are likely to disclose the information to overseas recipients and, if so, the countries in which these recipients are likely to be located;

g. what the consequences will be for the person if they do not provide the information to us;
h. how the person can access their personal information held by us; and
i. if we have obtained the information from someone else, or the individual may not be aware that we have collected the information, that we collect, or have collected, the information, and the circumstances of collection.

Special rule for health information or sensitive information?

As a general rule, we have to try harder to notify people when we're collecting health information or any information that might be considered sensitive.

Key messages, examples and definitions

Individuals providing their personal information to us have a right to know the full extent of how the information they provide will be used and disclosed, and to choose whether or not they wish to go ahead with providing information on that basis.

Notification therefore allows a person to make an informed decision about whether or not to give us their personal information. Notification is done through a 'privacy notice'.

Privacy notices can be given in writing or verbally, but writing is better. But we only need to take reasonable steps to ensure each person receives the notice.

Where the person lacks some capacity (e.g. because of a brain injury), we must notify their authorised representative, but also still try to communicate with the person direct.

To determine what might be "reasonable steps", we will consider:

the sensitivity of the information;

the possible uses of the information.

Common exemptions

Unsolicited information.

Information collected before 1 July 2000.

If another law authorises or requires us to not notify people.

Some law enforcement and investigation purposes.

The person has already been notified by the organisation that gave us the information.

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Other relevant points

When drafting a privacy notice, use the University's Template Privacy Notice attached in Appendix A to this document. Any new projects which might collect personal information should be reviewed by the University's Privacy Contact Officer to ensure an adequate privacy notice is included.

For non-English speaking background clients, the Community Language Privacy Notice should be used.

Privacy NSW's Best Practice Guide Privacy and people with decision-making disabilities explains how to notify a person who has limited capacity to understand.

Part G - Security Safeguards

(38) We will take reasonable security measures to protect personal information from loss, unauthorised access, use, modification or disclosure.

(39) We will ensure personal information is stored securely, not kept longer than necessary, and disposed of appropriately.

Special rule for health information or sensitive information?

As a general rule, we will have to work harder to protect health information or any information that might be considered sensitive.

Key messages, examples and definitions

Security measures could include technical, physical or administrative actions.

Example: We must only provide personal information to a contractor or service provider if they really need it to do their job. We must also take reasonable steps to prevent any unauthorised use or disclosure of the information by a contractor or service provider, and remember to bind our contractors to the same privacy obligations as us.

Example: We must follow good practice records management.

To determine what might be "reasonable steps", we will consider:

the sensitivity of the information;

the context in which the information was obtained;

the purpose for which we collected the information;

the possible uses of the information; and

the practicality and cost of aiming for 'best practice'.

Common exemptions

None.

Part H - Transparency

(40) We will enable anyone to know:

a. whether we are likely to hold their personal information;
b. the purposes for which we use personal information; and
c. how they can access their own personal information.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

We have a broad obligation to the community, to be open about how we handle personal information. This is different to collection notification, which is much more specific, and given at the time of collecting new personal information.

Example: This Plan will be available on our website. This Plan briefly explains our privacy obligations, and sets out the major categories of personal and health information that we hold.

Common exemptions

None.

Part I - Access

(41) We will allow people to access their personal information without unreasonable delay or unreasonable expense.

(42) We will only charge fees for access as permitted by the Government Information (Public Access) Act 2009 (refer Section 7 - of this Privacy Management Plan).

(43) We will only refuse access where authorised by law, and we will provide written reasons.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

People should be able to see what information we hold about them, with a minimum of fuss.

Our policy is that as much as possible, we will let both students and staff see their own personal information informally at no cost.

Where the University requires an access application be submitted formally, application and processing charges will apply.

Common exemptions

If another law (such as the Government Information (Public Access) Act 2009 (NSW)) authorises or requires us to not to give the person access.

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Other relevant points

Any unusual request to access personal information should be put in writing, and then referred to the University's Privacy Contact Officer for review.

Privacy NSW's Best Practice Guide Privacy and people with decision-making disabilities explains how to provide access to personal information held about a person who has limited or no capacity.

Part J - Correction

(44) We will allow people to update or amend their personal information to ensure it is accurate, relevant, up-to-date, complete or not misleading.

(45) We will suppress a person's address on request.

(46) Where possible, we will notify any other recipients of any changes.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

If we disagree with the person about whether the information needs changing, we must instead allow the person to add a statement to our records.

We can't charge people to lodge their request for amendment. But we can charge reasonable fees for making an amendment, if we tell people what the fees are up-front. Fees should be no more than we would charge for the same thing under the Government Information (Public Access) Act 2009 (NSW).

Our policy is, as much as possible, to let people update their own personal information at no cost. But this does not mean they can just ask us to alter their student grades without going through the proper processes.

Example: When a student calls or visits Student Services to obtain information about their course of study, or to change their personal details, or accesses Student One to update their contact details, the amendment process should be processed quickly and for no cost.

Common exemptions

If another law authorises or requires us to not amend the information.

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Other relevant points

Any unusual request to amend personal information should be put in writing, and then referred to the University's Privacy Contact Officer to review.

Part K - Accuracy

(47) Before using or disclosing personal information, we will take appropriate steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

We must ensure that personal information is still relevant and accurate before we use or disclose it.

We only need to take reasonable steps to check the information - but more steps will be needed if we're likely to use the information in a way that will disadvantage the person.

What might be considered "reasonable steps" will depend upon the circumstances, but some points to consider are:

the context in which the information was obtained;

the purpose for which we collected the information;

the purpose for which we now want to use the information;

the sensitivity of the information;

the number of people who will have access to the information;

the potential effects for the person if the information is inaccurate or irrelevant;

any opportunities we've already given the person to correct inaccuracies; and

the effort and cost involved in checking the information.

Example: When Enrolment services are determining a potential student's eligibility to study with us, we will give the person an opportunity to correct the information we are relying on before we make our final decision. The same process applies to any information about students or staff published by the University's Communications Media and Marketing department.

Common exemptions

None.

Part L - Use

(48) We may use personal information:

a. for the primary purpose for which it was collected;
b. for a directly related secondary purpose within the reasonable expectations of the person; or
c. for another purpose if the person has consented.

Special rule for health information or sensitive information?

No.

Key messages, examples and definitions

We should only use personal information for the purpose for which it was collected. We shouldn't go finding new and interesting uses for people's personal information.

Example: If the primary purpose of collecting student information was to process an enrolment and course selection, directly related secondary purposes within the reasonable expectations of the person for which their personal information could be used by the University would include billing for the course, auditing or course evaluation.

Common exemptions

To deal with a serious and imminent threat to any person.

If another law authorises or requires us to use the information.

Some law enforcement and investigative purposes.

Some research purposes, subject to approval by the University's Human Research Ethics Committee.

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Other relevant points

The primary purpose for which we have collected the information should have been set out in a privacy notice. To use personal information for a purpose set out in the privacy notice is usually OK, but for any other purpose, check with the University's Privacy Contact Officer first.

Privacy NSW's Best Practice Guide Privacy and people with decision-making disabilities explains how to seek consent for a secondary use of personal information from a person who has limited or no capacity.

Privacy NSW's Statutory Guidelines on Research explain how health information can be used for research purposes. It also provides a good rule of thumb for the use of other types of personal information for research purposes.

Part M - Disclosure

(49) We will only disclose personal information if:

a. at the time we collected their information, the person was given a privacy notice to inform them their personal information would or might be disclosed to the proposed recipient;
b. the disclosure is directly related to the purpose for which the information was collected, and the University has no reason to believe that the individual concerned would object to the disclosure; or
c. the person concerned has consented to the proposed disclosure.

Special rule for health information or sensitive information?

Yes. If the personal information is 'sensitive personal information', we may only disclose it if the person has consented.

Tougher rules also apply when transferring health information outside of NSW (including to the Commonwealth Government). We can only transfer health information outside NSW if one of the following applies:

a. the person concerned has consented;
b. if it is necessary for a contract with (or in the interests of) the person concerned;
c. if it will benefit the person concerned, we cannot obtain their consent, but we believe the person would be likely to give their consent;
d. we reasonably believe that the recipient of the information is subject to a law or binding scheme equivalent to the HPPs; or
e. we have bound the recipient by contract to privacy obligations equivalent to the HPPs.

Key messages, examples and definitions

So long as the personal information in question is not 'sensitive personal information', we can disclose information in ways we clearly notified the person about at the time we collected their personal information.

However if we didn't tell the person about the proposed disclosure in a privacy notice, or if the personal information in question is 'sensitive personal information', or if it is health information and we want to send it outside NSW, we will usually have to get the person's consent for the disclosure.

Common exemptions

To deal with a serious and imminent threat to any person

To deal with a serious threat to public health or safety (health information only)

If another law authorises or requires us to disclose the information

Some law enforcement and investigative purposes

Some research purposes, subject to approval by the University's Human Research Ethics Committee.

Before you rely on an exemption, check with the University's Privacy Contact Officer.

Other relevant points

The primary purpose for which we have collected the information should have been set out in a privacy

notice. To disclose personal information that is not 'sensitive' for a purpose set out in the privacy notice is usually OK, but for any other purpose, check with the University's Privacy Contact Officer first.

Privacy NSW's Best Practice Guide Privacy and people with decision-making disabilities explains how to seek consent for a disclosure of personal information from a person who has limited or no capacity.

Privacy NSW's Statutory Guidelines on Research explain how health information can be disclosed for research purposes. It also provides a good rule of thumb for the disclosure of other types of personal information for research purposes.

Section 5 - Information Subject to the Privacy Act 1988 (Cth)

(50) Information defined at clause (17) which is subject to the provision of the Privacy Act 1988 (Cth) will be managed in accordance with the principles contained in this Plan and:

a. where the University receives unsolicited personal information:
    i. the University will, within a reasonable period, determine whether it could have collected the information under APP 3;
    ii. if the information could have been collected, then APPs 5 to 13 apply to the information;
    iii. if the University could not have collected the information, it will destroy or de-identify the information as soon as practicable, but only if lawful and reasonable to do so;
b. the University will not disclose personal information to an overseas recipient, unless:
    i. the University is reasonably satisfied the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that is at least substantially similar to the way in which the APPs protect the information, and there are mechanisms that the individual can access to take action to enforce that protection; or
    ii. the individual has provided their consent to the cross-border disclosure; or
    iii. it is required under law;
c. the University will only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt-out mechanisms are met.

Section 6 - Privacy Complaints

(51) Students and staff of the University may lodge an informal complaint by contacting the unit concerned. If a privacy complaint cannot be resolved informally by the unit concerned, a person may apply for an 'internal review' of conduct they believe breaches an IPP, HPP and/or an APP.

(52) Internal review is the process by which the University manages formal, written privacy complaints about how we have dealt with personal information or health information. All written complaints about privacy are considered to be an application for internal review, even if the applicant doesn't use the words 'internal review'.

(53) By law, an application for internal review must:

a. be in writing;
b. be addressed to the University;
c. specify an address in Australia to which the applicant is to be notified after the completion of the review; and
d. be lodged at the University within six months from the time the applicant first became aware of the conduct that they want reviewed.

(54) The University encourages the use of the Internal Review Application Form, found at Appendix B to this Plan.

(55) An application for internal review can be on behalf of someone else.

(56) Where the applicant is not literate in either English or their first language and where there is no other organisation making the application on their behalf, staff should help the person to write their application. Staff should use a professional interpreter, if necessary. Applications in other languages will be accepted and translated, and all acknowledgments and correspondence to the applicant will be translated.

(57) Students and staff of the University may make a request for internal review and investigation through contact with the University's Privacy Contact Officer.

(58) Applications for internal review, or any written complaint about privacy, received at any the University office, should be forwarded immediately to the University's Privacy Contact Officer who can be reached as follows:

The SCU Privacy Contact Officer
SCU Legal Office
Southern Cross University
PO Box 157
LISMORE
PH: (02) 6620 3465
Fax: (02) 6626 9125
Email: privacy@scu.edu.au

(59) If the Privacy Contact Officer decides that the complaint is about an alleged breach of the IPPs, HPPs and/or APPs, the internal review will be conducted by the Privacy Contact Officer or another staff member who:

a. was not involved in the conduct which is the subject of the complaint;
b. is an employee or an officer of the agency, and
c. is qualified to deal with the subject matter of the complaint.

Extensions of time for lodgement

(60) While the legislation allows applicants six months to apply for an internal review from the time the applicant first becomes aware of the conduct, the University may accept late applications.

(61) Possible acceptable reasons for delay may be:

a. ill-health or other reasons relating to capacity;
b. the complainant only recently becoming aware of his or her right to seek an internal review; or
c. the complainant reasonably believing that he or she would suffer ill-effects as a result of making an application at an earlier time.

(62) However late applications that, because of their age, cannot be investigated in a meaningful way will be declined. In these cases, witnesses may no longer be available, documents may have been destroyed and memories may have faded.

(63) Final decisions on the acceptance of late applicants will only be made by the University's Privacy Contact Officer. Where the University declines to accept an application because it is too old, the reason will be explained in a letter to the applicant.

The Internal Review process

(64) When the University receives an internal review application, the Privacy Contact Officer will:

a. 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; and
b. send a letter to the NSW Privacy Commissioner with details of the application. A photocopy of the written complaint will also be provided to the NSW Privacy Commissioner.

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

(66) 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 our preliminary determination to the IPC,

(67) When the internal review is completed, and the University has received a response from the Privacy Commissioner about our draft preliminary determination, the University's Privacy Contact Officer 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 and/or APPs;
c. any action we propose 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 NSW Civil and Administrative Tribunal.

(68) We will also send a copy of this letter to the Privacy Commissioner.

(69) Statistical information about the number of internal reviews conducted must be maintained for the University's Annual Report.

External review by the NSW Civil and Administrative Tribunal

(70) People may apply to the NSW Civil and Administrative Tribunal for an external review of the conduct which was the subject of their earlier internal review application. The NSW Civil and Administrative Tribunal may make orders requiring the University to:

a. refrain from conduct or action which breaches an IPP, HPP or Code;
b. perform in compliance with an IPP, HPP or Code;
c. correct information disclosed by the University; or
d. take steps to remedy loss or damage.

(71) The NSW Civil and Administrative Tribunal may also make an order requiring the University to pay damages of up to $40,000 if the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

Section 7 - Fees and Charges

(72) The University will impose fees for formal information access applications. When determining the fee amount, we will use applicable provisions of the Government Information (Public Access) Act 2009 which are currently as follows:

Activity	Cost
Information Access Application Fee	$30
Processing Fee	$30 per hour - (applicant gets 20 hours free when seeking their own personal information - other discounts may apply).

Status and Details

Status	Historic
Effective Date	12th September 2014
Review Date	12th May 2017
Approval Authority	Vice Chancellor
Approval Date	12th September 2014
Expiry Date	14th April 2015
Head of Work Unit	Mark Dixon Director, Governance Services
Enquiries Contact	Governance Services