

Privacy Management Plan

Section 1 - Introduction

About this Privacy Management Plan

- (1) The purpose of this Privacy Management Plan (PMP) is two-fold.
- (2) Firstly, this Plan demonstrates to members of the public how SCU upholds and respects the privacy of the students, staff and others about whom we hold personal information.
- (3) Secondly, this Plan - particularly Section 4 and the Privacy Notice and Consent Wording Template - acts as a reference tool for SCU staff, to explain how we may best meet our privacy obligations under the Privacy and Personal Information Protection Act 1998 (NSW) and the [Health Records and Information Privacy Act 2002 \(NSW\)](#).

Introduction to SCU and its privacy context

- (4) Southern Cross University (SCU) is an Australian public university established and operating under the [Southern Cross University Act 1993 \(NSW\)](#). SCU has more than 15,000 students studying on its campuses and through education collaborations within Australia and 60 countries around the world. More than 3,000 postgraduate students undertake their degrees with Southern Cross University across a broad suite of disciplines.
- (5) Areas of teaching specialisation include tourism, business and information technology, environmental science and management, education, the humanities, legal and justice studies and the creative and performing arts. Research strengths include plant genetics, biofuels, change innovation and organisational development, and health promotion and disease prevention.
- (6) Due to the nature of our work, SCU holds a vast amount of personal information not only pertaining to the students we serve, but also relating to our staff. SCU takes the privacy of our students and staff seriously, and we will protect privacy with the use of this Privacy Management Plan as a reference and guidance tool.
- (7) As a NSW public sector agency, SCU is regulated by the Privacy and Personal Information Protection Act 1998 (the PPIP Act) and the [Health Records and Information Privacy Act 2001](#) (HRIP Act).
- (8) Both of these Acts centre around what are termed 'privacy principles'. The PPIP Act covers personal information other than health information, and requires agencies 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.
- (9) Health information is regulated by a slightly different set of principles. 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 SCU 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.

- (10) There are exemptions to many of the privacy principles, found in the two Acts themselves, and in Regulations,

Privacy Codes and Public Interest Directions.

(11) Both the PPIP Act and the [HRIP Act](#) contain criminal offence provisions applicable to employees of SCU who use or disclose personal information or health information without authority. SCU is also subject to confidentiality provisions in the contracts through which we arrange our educational collaborations.

The SCU Privacy Contact Officer

SCU Legal Services

Southern Cross University

PO Box 157

LISMORE

PH: (02) 6620 3465

Fax: (02) 6626 9125

Email: privacy@scu.edu.au

Section 2 - Types of personal and health information held

(12) Examples of personal information held by SCU 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 SCU's School of Natural and Complementary Medicine, and of individuals associated with the clinical placements of students in the Health Sciences faculty:
- 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.

Section 3 - Inventory of Signification Information Systems

System	Purpose
Academic Integrity Database:	Excel-based database maintained by Performance Quality Review (PQR) for registration and monitoring of current and past academic integrity issues.
Aurion	Human Resources information database (including some payroll capacity).
CHORUS:	Database used by the Relations Development Unit to capture and store information about the commercial and other relationships it supports.
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, particularly the Office to Assist Student Involvement and Success (OASIS) and the Office of Sport and Cultural Activities (OSCA).
Finance One:	SCU's core finance system.
MIS:	Management Information System
SONIA:	Clinical placements database used specifically for storage of information relating to midwifery projects, superseded by CONRAD.
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 - How the privacy principles apply

How the privacy principles apply

(13) The privacy principles are the standards which SCU is expected to follow when dealing with personal information (including health information).

(14) The phrase 'privacy principles' refers to the combination of the 12 Information Protection Principles (IPPs) set out in sections 8 to 19 of the Privacy and Personal Information Protection Act 1998, and the 15 health privacy principles (HPPs) in Schedule 1 of the [Health Records and Information Privacy Act 2002](#) (HRIP Act).

(15) There are a number of ways that our conduct may be exempt from one or more of the IPPs or HPPs. 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.

(16) The following section uses plain language (not the wording of the law itself) to describe the privacy principles and how SCU staff must comply with them. It also mentions the exemptions that may be relevant for SCU, depending on the context. If you need guidance on interpreting the requirements of the privacy principles or exemptions, please contact SCU's Privacy Contact Officer.

Introduction

(17) Our privacy obligations have been condensed into one set of 13 plain language principles to be followed by SCU:

1. limiting our collection of personal information;
2. anonymity;
3. unique identifiers;
4. how we collect personal information - the source;
5. how we collect personal information - the method and content;
6. notification when collecting personal information;
7. security safeguards;
8. transparency;
9. access;
10. correction;

11. accuracy;

12. use; and

13. disclosure.

(18) This Section of the PMP outlines:

- a. key definitions;
- b. each of the SCU plain language privacy principles;
- c. when there are different rules for 'health information' or 'sensitive personal information';
- d. some examples of how the privacy principles work in practice; and
- e. the common exemptions to each privacy principle.

Important note about using this section

(19) This Section of the PMP uses plain language, not the exact wording of the law. This is to make understanding our obligations a little easier. This document does not cover the full complexity of the privacy laws applying to SCU. It has been simplified, and doesn't cover all exemptions or situations.

(20) If in doubt, you should always check the exact wording in the legislation, and seek guidance from the SCU Privacy Contact Officer, or the NSW Privacy Commissioner.

(21) This document is an educational tool, not legal advice.

Definitions

(22) "Collection" of personal information means the way SCU 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.

(23) "Disclosure" means when we provide personal information to an individual or body outside SCU - or, in some cases, to other discrete units within SCU.

(24) "Health information" means personal information that is also information or an opinion about:

- a. a person's physical or mental health or disability
- b. a health service provided, or to be provided, to a person
- c. a person's express wishes about the future provision of health services to him or her
- d. 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
- e. genetic information that is or could be predictive of the health of a person or their relatives or descendants.

(25) "Holding" personal information: SCU will be considered to be 'holding' personal information if it is in SCU'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 SCU is 'holding' personal information, which means we remain responsible for what our contractors or service providers do on our behalf.

(26) "Personal information" means "information or an opinion ... about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion".

(27) 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.

(28) 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.

(29) 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.

(30) "Privacy obligations" means the privacy principles and any exemptions to those principles that apply to SCU.

(31) "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.

(32) "Use" means when SCU uses personal information for some purpose.

Principle 1 - Limiting our collection of personal information

1.1 The principle in brief

(33) 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.

1.2 Special rule for health information or sensitive information?

(34) No.

1.3 Key messages, examples and definitions

(35) 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.

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

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

(38) 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.

1.4 Common exemptions

(39) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. unsolicited information
- b. information collected before 1 July 2000

Principle 2 - Anonymity

2.1 The principle in brief

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

2.2 Special rule for health information or sensitive information?

(41) No.

2.3 Key messages, examples and definitions

(42) Example: Potential 'customers' of SCU should be provided with information about SCU's programs and services, without having to identify themselves.

2.4 Common exemptions

(43) None.

Principle 3 - Unique identifiers

3.1 The principle in brief

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

3.2 Special rule for health information or sensitive information?

(45) No.

3.3 Key messages, examples and definitions

(46) 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.

(47) 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'.

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

3.4 Common exemptions

(49) None.

Principle 4 - How we collect personal information - the source

4.1 The principle in brief

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

4.2 Special rule for health information or sensitive information?

(51) 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.

4.3 Key messages, examples and definitions

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

(53) 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.

(54) Example: An SCU 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.

(55) Example: Potential students have already authorised UAC to provide their information to SCU on their behalf, when applying for a course at SCU.

4.4 Common exemptions

(56) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. unsolicited information
- b. where the person is under 16, we can instead collect the information from their parent or guardian (but we don't have to)
- c. if another law authorises or requires us to collect the information indirectly (i.e. from a different source)
- d. for some law enforcement and investigation purposes
- e. when we are taking a family, social or medical history from a client of our health or counselling services
- f. information collected before 1 July 2000
- g. if compliance would, in the circumstances, prejudice the interests of the individual to whom the information relates.

4.5 Other relevant points

(57) 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.

(58) 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.

Principle 5 - How we collect personal information - the method and content

5.1 The principle in brief

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

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

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

5.2 Special rule for health information or sensitive information?

(62) No.

5.3 Key messages, examples and definitions

(63) 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.

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

- a. the sensitivity of the information;
- b. the possible uses of the information; and
- c. the practicality and cost of aiming for 'best practice'.

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

5.4 Common exemptions

(66) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. unsolicited information
- b. information collected before 1 July 2000

Principle 6 - Notification when collecting personal information

6.1 The principle in brief

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

- a. who will hold and/or have access to their personal information;
- b. what it will be used for;
- c. what other organisations (if any) routinely receive this type of personal information from us;
- d. whether the collection is required by law;
- e. what the consequences will be for the person if they do not provide the information to us; and
- f. how the person can access their personal information held by us.

6.2 Special rule for health information or sensitive information?

(68) 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.

6.3 Key messages, examples and definitions

(69) Individuals providing their personal information to SCU 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.

(70) 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'.

(71) 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.

(72) 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.

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

- a. the sensitivity of the information;
- b. the possible uses of the information; and
- c. the practicality and cost of aiming for 'best practice'.

6.4 Common exemptions

(74) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. unsolicited information
- b. information collected before 1 July 2000
- c. if another law authorises or requires us to not notify people
- d. some law enforcement and investigation purposes
- e. the person has already been notified by the organisation that gave us the information

6.5 Other relevant points

(75) When drafting a privacy notice, use the SCU Privacy Notice and Consent Wording Template. Any new projects which might collect personal information should be reviewed by the SCU Privacy Contact Officer to ensure an adequate privacy notice is included.

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

(77) [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.

Principle 7 - Security safeguards

7.1 The principle in brief

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

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

7.2 Special rule for health information or sensitive information?

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

7.3 Key messages, examples and definitions

(81) Security measures could include technical, physical or administrative actions.

(82) 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.

(83) Example: We must follow good practice records management.

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

- a. the sensitivity of the information;
- b. the context in which the information was obtained;
- c. the purpose for which we collected the information;
- d. the possible uses of the information; and
- e. the practicality and cost of aiming for 'best practice'.

7.4 Common exemptions

(85) None.

Principle 8 - Transparency

8.1 The principle in brief

(86) 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.

8.2 Special rule for health information or sensitive information?

(87) No.

8.3 Key messages, examples and definitions

(88) 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.

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

8.4 Common exemptions

(90) None.

Principle 9 - Access

9.1 The principle in brief

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

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

9.2 Special rule for health information or sensitive information?

(93) No.

9.3 Key messages, examples and definitions

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

(95) Our policy is that as much as possible, we will let both students and staff see their own personal information at no

cost, and through an informal request process.

(96) We can't charge people to lodge their request for access. But we can charge reasonable fees for copying or inspection, 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).

9.4 Common exemptions

(97) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. if another law (such as the [Government Information \(Public Access\) Act 2009](#) (NSW)) authorises or requires us to not to give the person access.

9.5 Other relevant points

(98) Any unusual request to access personal information should be put in writing, and then referred to the SCU Privacy Contact Officer to review.

(99) [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.

Principle 10 - Correction

10.1 The principle in brief

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

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

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

10.2 Special rule for health information or sensitive information?

(103) No.

10.3 Key messages, examples and definitions

(104) 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.

(105) 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).

(106) 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.

(107) 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.

10.4 Common exemptions

(108) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. if another law authorises or requires us to not to amend the information.

10.5 Other relevant points

(109) Any unusual request to amend personal information should be put in writing, and then referred to the SCU Privacy Contact Officer to review.

Principle 11 - Accuracy

11.1 The principle in brief

(110) 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.

11.2 Special rule for health information or sensitive information?

(111) No.

11.3 Key messages, examples and definitions

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

(113) 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.

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

- a. the context in which the information was obtained;
- b. the purpose for which we collected the information;
- c. the purpose for which we now want to use the information;
- d. the sensitivity of the information;
- e. the number of people who will have access to the information;
- f. the potential effects for the person if the information is inaccurate or irrelevant;
- g. any opportunities we've already given the person to correct inaccuracies; and
- h. the effort and cost involved in checking the information.

(115) 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 SCU's Communications and Publications department.

11.4 Common exemptions

(116) None.

Principle 12 - Use

12.1 The principle in brief

(117) 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.

12.2 Special rule for health information or sensitive information?

(118) No.

12.3 Key messages, examples and definitions

(119) 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.

(120) 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 SCU would include billing for the course, auditing or course evaluation.

12.4 Common exemptions

(121) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. to deal with a serious and imminent threat to any person
- b. if another law authorises or requires us to use the information
- c. some law enforcement and investigative purposes
- d. some research purposes, subject to approval by the SCU Human Research Ethics Committee.

12.5 Other relevant points

(122) 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 SCU Privacy Contact Officer first.

(123) [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.

(124) [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.

Principle 13 - Disclosure

13.1 The principle in brief

(125) 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 SCU 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.

13.2 Special rule for health information or sensitive information?

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

consented.

(127) 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.

13.3 Key messages, examples and definitions

(128) 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.

(129) 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.

13.4 Common exemptions

(130) Before you rely on an exemption, check with the SCU Privacy Contact Officer.

- a. to deal with a serious and imminent threat to any person
- b. to deal with a serious threat to public health or safety (health information only)
- c. if another law authorises or requires us to disclose the information
- d. some law enforcement and investigative purposes
- e. some research purposes, subject to approval by the SCU Human Research Ethics Committee.

13.5 Other relevant points

(131) 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 SCU Privacy Contact Officer first.

(132) [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.

(133) [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 - Privacy Complaints

(134) Students and staff of SCU 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 and/or an HPP.

(135) Internal review is the process by which SCU 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'.

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

- a. be in writing;
- b. be addressed to SCU;
- 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 SCU within six months from the time the applicant first became aware of the conduct that they want reviewed.

(137) SCU encourages the use of the Internal Review Application Form.

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

(139) 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.

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

(141) Applications for internal review, or any written complaint about privacy, received at any SCU office, should be forwarded immediately to the SCU's Privacy Contact Officer who can be reached on (02) 6620 3465 or via email at privacy@scu.edu.au

(142) If the Privacy Contact Officer decides that the complaint is about an alleged breach of the IPPs and/or HPPs, 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

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

(144) 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.

(145) 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.

(146) Final decisions on the acceptance of late applicants will only be made by the SCU Privacy Contact Officer. Where

the decision is made not to accept an application because it is too old, the reason will be explained in a letter to the applicant.

The Internal Review process

(147) When SCU 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 Administrative Decisions 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 Privacy Commissioner.

(148) Internal reviews follow the process set out in the Privacy NSW Internal Review Checklist .

(149) When the internal review is completed the SCU 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 and/or HPPs;
- 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 Administrative Decisions Tribunal.

(150) We will also send a copy of this letter to the [Privacy Commissioner](#).

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

External review by the Administrative Decisions Tribunal

(152) People may apply to the Administrative Decisions Tribunal for an external review of the conduct which was the subject of their earlier internal review application. The Tribunal may make orders requiring SCU 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 SCU; or
- d. take steps to remedy loss or damage.

(153) The Tribunal may also make an order requiring SCU 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.

Status and Details

Status	Historic
Effective Date	14th August 2012
Review Date	14th April 2015
Approval Authority	Vice Chancellor
Approval Date	10th August 2012
Expiry Date	17th March 2014
Head of Work Unit	Mark Dixon Director, Governance Services
Enquiries Contact	Mark Dixon Director, Governance Services