PRIVACY PROCEDURES 2018

Issued by:	General Counsel
Dated:	20 April 2018
Last amended:	18 June 2018
Signature:	
Name:	Mr Richard Fisher, AM

---

1 Purpose and application

(1) These procedures are to give effect to the *Privacy Policy 2017* ("the policy").

(2) These procedures apply to the University, staff, students and affiliates.

(3) These procedures do not apply to:

(a) requests for information made under the *Government Information (Public Access) Act 2009 (NSW)*; or

(b) applications to access information under the *Privacy and Personal Information Act 1988 (NSW)*.

(4) Part 1 of these procedures deals with the disclosure of personal information to third parties.

(5) Part 2 of these procedures detail how the University will manage a notifiable privacy breach involving personal and/or health information held by the University.

2 Commencement

These procedures commence on 1 May 2018.

3 Interpretation

(1) Words and phrases used in these procedures and not otherwise defined in this document have the meanings they have in the policy.

consent	means agreement, which is: • given by an individual who has the capacity to understand and communicate it; • voluntary; • informed; • specific; and • current.
disclosure	means providing an individual's personal information to another person or entity, generally a person or entity outside of the University.
express consent	means consent that is: • clearly and unmistakably communicated; • precise about the kind and, if possible, exact contents of the information to which it relates; and • precise about to whom the information may be disclosed.
health information	means the type of personal information defined as such in section 6 of the *Health Records and Information Privacy Act 2002* (NSW). It may include, but is not limited to: • information about an individual's physical or mental health or, disability; • blood or DNA samples; • information about a health service provided to an individual; • information or opinions about an individual's physical or mental health, or disability.
held	means information that is in the possession or control of the University's staff or affiliates. This includes where staff or affiliates physically possess the information and also where they have the right or power to deal with it.
implied consent	means consent that can reasonably be inferred from an individual's actions.
law enforcement agency	has the meaning provided in section 3 of the *Privacy and Personal Information Protection Act 1998* (NSW) which at the date of these procedures is any of: • the New South Wales Police Force or the police force of any other State or Territory • the New South Wales Crime Commission • the Australian Federal Police • the Australian Crime Commission • the Director of Public Prosecutions of New South Wales or of another State or Territory, or of the Commonwealth • the Department of Justice • the office of the Sherriff of New South Wales

- a person or body prescribed by the regulations for the purposes of this definition.

personal information	has the meaning given in section 4 of the *Privacy and Personal Information Protection Act 1998 (NSW)*, excluding subsection 4(3)(j) of that Act. It includes any information or opinion about a person where their identity is apparent or can reasonably be ascertained, such as • an individual's name; • an individual's address; • an individual's student or staff number; • CCTV and other video recordings of an individual; and • information or an opinion about an individual's suitability for employment or promotion at the University. In these procedures references to personal information also include health information.
privacy acts	means either or both of the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW)
privacy breach	means a situation where personal or health information held by the University is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference.
Proper Officer	means the person appointed to receive subpoenas on behalf of the University. At the time of these procedures' commencement, it is the University's Records Manager.
real risk of serious harm	has the meaning given by clause 16 of these procedures.

PART 1 - DISCLOSURE OF PERSONAL INFORMATION TO THIRD PARTIES

4 Disclosure of personal information generally

(1) The University will only disclose personal information that it holds about an individual if:

(a) the individual to whom the information relates has given their express consent;

Note: An individual cannot give express consent in advance to disclosure of information which does not exist, or is unknown, at the time consent is sought.

(b) the disclosure is required or authorised by law;

(c) the disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the individual would object;

(d) the individual has been made aware, or is reasonably likely to have been aware, that information of that kind is usually disclosed;

(e) in the case of health information, and in accordance with the relevant statutory guidelines, it is reasonably necessary for the management of health services, training or research or it is being used for a related health treatment; or

(f) one of more of clauses 5 – 12 of these procedures applies.

(2) The University will only disclose personal information that it holds about an individual which relates to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities if:

(a) the individual has given their express consent;

(b) the University reasonably believes that it is necessary to prevent a serious or imminent threat to any person's life or health; or

(c) the disclosure is required or authorised by law.

5 Disclosure in cases of emergency

(1) The University may disclose an individual's personal information without their consent where disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

(2) The University may disclose health information without an individual's consent if it is necessary to find a missing person.

(3) Decisions to disclose information in relation to subclauses 5(1) and 5(2) of these procedures are made as follows:

(a) relating to students: by the Deputy Vice-Chancellor (Registrar) or Director; Student Services

(b) relating to staff members: by the Chief Human Resources Officer;

(c) relating to members of the public: by the Group Secretary.

6 Disclosure to government agencies

(1) As required by law, the University may disclose the personal information of staff, affiliates and students to government agencies with responsibilities for social security and human services, national security, immigration and taxation.

(2) If there is no pre-existing administrative arrangement between the University and a government agency, disclosure may only occur in response to a formal written notice or request under the agency's legislation.

(3) Staff or affiliates who receive a non-routine request for personal information from a government agency must contact the University's Privacy Officer before responding.

Note: Use: privacy.enquiries@sydney.edu.au.

7 Disclosure under subpoenas, warrants or other court orders

(1) Staff or affiliates who receive subpoenas, warrants or other court orders must forward them to the University's Proper Officer who will manage the response.

(2) Staff and affiliates must co-operate with any requests from the University's Proper Officer as part of the University's response to a subpoena or warrant.

8 Disclosure to law enforcement agencies

(1) Except in emergencies, a staff member or affiliate who receives a request (whether in person, written or over the phone) for personal information from a law enforcement officer or agency must forward it to the University's Proper Officer who will manage the response.

(2) In cases other than an emergency, decisions to disclose information to law enforcement officers or agencies are made as follows:

(a) relating to students: by the Deputy Vice-Chancellor (Registrar) or Director; Student Services;

(b) relating to staff members: by the Chief Human Resources Officer;

(c) relating to members of the public: by the Group Secretary.

9 Disclosure of closed circuit television (CCTV) vision

(1) The University will only disclose CCTV vision that includes personal information (e.g. images of individuals) in accordance with clause 4 of these procedures.

(2) Except in emergencies, the University's Proper Officer will manage disclosure of CCTV vision to a law enforcement agency.

10 Disclosure to external service providers

Where an external service provider has access to personal information held by the University, the agreement under which the service provider is engaged must contain:

(a) a detailed description of the personal information that is to be provided to the service provider; and

(b) where the service provider holds personal information obtained in the course of the engagement:

(i) a requirement that the personal information be returned or securely destroyed at the end of the engagement; and

(ii) specification of the manner in which it may be returned or destroyed.

Note: Standard agreements containing these requirements are found here: https://intranet.sydney.edu.au/services/buying-leasing-paying/buying/templates.html

11 Disclosure for research purposes

(1) Staff, affiliates or students seeking to use or disclose health information or personal information for research purposes without the relevant individual's consent must

comply with the relevant statutory guidelines issued by the NSW Privacy Commissioner.

Note: See: *Statutory Guidelines on Research Health Records and Information Privacy Act (2002) NSW* and *Statutory Guidelines on Research section 27B Privacy and Personal Information Protection Act 1988 (NSW)*.

(2) Staff or students engaged in research subject to a grant from the National Health & Medical Research Council or the Australian Research Council, and who seek to use or disclose health or personal information, must comply with the relevant statutory guidelines approved by the Commonwealth Privacy Commissioner.

Note: See: *Guidelines under section 95 of the Privacy Act 1988* and *Guidelines approved under section 95A of the Privacy Act 1988*.

12 Disclosure to other third parties

(1) The University will not disclose personal information without one or more of:

(a) the express consent of the subject of the information;

(b) being required or authorised by law to do so; or

(c) being properly served with a subpoena or similar court order to do so.

(2) Staff or affiliates who receive requests from solicitors or insurance companies should direct these to the University's Proper Officer.

(3) Requests about deceased individuals should be directed to the University's Proper Officer.

(4) Staff or affiliates must not provide a reference, for example for an employment application, unless the individual the subject of that reference:

(a) has requested a reference; or

(b) has given consent to the disclosure of their personal information.

(5) The University will only disclose personal information of students who are minors to their parents or guardians in accordance with the privacy acts, the policy and these procedures.

(a) Third parties concerned that there may be a serious and imminent threat to life or health of a student should be directed to the University's Student Support Services.

13 Unauthorised disclosure

(1) Staff, affiliates or students who become aware of an unauthorised disclosure of personal information involving an information or communications technology resource must immediately report it to the ICT Helpdesk.

Note: Use ict.support@sydney.edu.au or (02) 9351 6000.

(2) Information and Communications Technology staff must notify the Manager, ARMS of any actual or potential unauthorised disclosure of personal information as soon as possible after becoming aware of it.

(3) Notifiable privacy breaches will be managed by in accordance with Part 2 of these procedures.

THE UNIVERSITY OF SYDNEY

PART 2 - NOTIFIABLE PRIVACY BREACHES

14 Notifiable privacy breaches generally

(1) A notifiable privacy breach is a breach that requires notification to one or more of:

(a) external stakeholders, such as the NSW Privacy Commissioner or the Commonwealth Privacy Commissioner; or

(b) internal stakeholders, such as those impacted by the breach and other University stakeholders.

(2) A notifiable privacy breach involves one or more of:

(a) a real risk of serious harm to those impacted by it;

(b) ongoing consequences, or the risk of ongoing consequences in terms of the number of people who may be impacted;

(c) the potential for serious reputational damage to the University; or

(d) the potential for legal or financial penalties to the University.

(3) The Manager, ARMS will determine whom to notify in cases of notifiable privacy breaches.

15 Initial assessment of suspected notifiable privacy breaches

(1) Upon being informed of a suspected breach, the Manager, ARMS will assess the situation and determine whether a breach has occurred.

(2) In doing so the Manager, ARMS may, as necessary:

(a) convene discussions with relevant stakeholders; and

(b) collate and review any relevant information.

(3) Where reasonable, the assessment and determination must be completed within 10 business days.

(4) The Manager, ARMS will notify the Group Secretary and General Counsel of the determination, and reasons for it, as soon as possible.

16 Real risk of serious harm

(1) In assessing whether there is a real risk of serious harm, the Manager ARMS must take into account the matters specified in this clause.

(2) Harm includes physical, financial or psychological harm. This may include the possibility of any or all of:

(a) identity theft;

(b) financial fraud; or

(c) misuse of health information;

leading to embarrassment, discrimination, or in extreme cases, blackmail.

(3) The following matters must be considered:

(a) whether the data is of a kind likely to cause individual harm if it is compromised: for example, health information, financial account information such as credit or debit card numbers, and government identifiers such as Medicare card numbers and driver's licence numbers;

(b) whether the situation involves the possibility of a combination of personal information creating a greater risk; and

(c) whether the information is permanent or temporary. A permanent piece of information such as a name, date of birth and medical history cannot be re-issued.

17 Breach response process

(1) The Manager, ARMS will co-ordinate the response to a notifiable privacy breach. This includes any formal management response or required approvals.

(2) A response to a notifiable privacy breach must involve each of :

(a) identifying the extent of the impact of the breach;

(b) containing or mitigating the impact;

(c) investigating the root cause;

(d) remediating the breach;

(e) taking steps to prevent future breaches; and

(f) notifying internal and external stakeholders.

18 Breach report

(1) The Manager, ARMS must prepare a written report on each notifiable breach as soon as possible after completing the breach response process.

(2) The report must set out:

(a) a chronology of all relevant events; and

(b) a summary of all steps taken in response.

(3) Copies of the report must be provided to the Group Secretary and the General Counsel.

(4) A copy of the report must be recorded in the University's recordkeeping system.

Note: See *Recordkeeping Policy 2017*.

NOTES

Privacy Procedures 2017

Date adopted:	20 April 2018
Date commenced:	1 May 2018
Date amended:	18 June 2018
Administrator:	Manager, Archives and Records Management Services
Review date:	20 April 2023
Rescinded documents:	
Related documents:	*Privacy and Personal Information Protection Act 1998* (NSW)
	Health Records and Information Privacy Act 2002 (NSW)
	Privacy Policy 2017

AMENDMENT HISTORY

Provision	Amendment	Commencing
14(2)(b)	Update 14(2)(b) to reflect 9(2)(b) of the *Privacy Policy 2017*	18 June 2018