PRIVACY POLICY 2017

The General Counsel, as delegate of the Senate of the University of Sydney, adopts the following policy.

Dated: 15 December 2017

Last amended: 13 June 2023 (administrative amendments)

20 December 2023 (administrative amendments)

Commencing: 24 April 2018

13 June 2023

20 December 2023

Current policy approver: Chief Governance Officer

CONTENTS

1 Name of policy

This is the Privacy Policy 2017.

2 Commencement

This policy commences on 24 April 2018.

3 Policy is binding

Except to the extent that a contrary intention is expressed, this policy binds the University, staff, students and affiliates.

4 Statement of intent

This policy:

(a) states the University's commitment to protecting privacy, in compliance with its legal and regulatory obligations;

(b) provides for the appropriate and compliant management of personal and health information;

(c) sets out the privacy responsibilities of the University, its staff, students and affiliates; and

(d) meets the statutory requirement for the preparation and implementation of a University privacy management plan.

5 Application

This policy applies to the University, staff, students and affiliates.

6 Definitions

data breach	has the meaning given in clause 7 of the *Data Breach Policy 2023* which at the date of this policy means: when personal or health information held by the University has been: • unlawfully accessed; • improperly shared; • lost; • accidentally or unlawfully destroyed; or • deliberately altered with intent to misrepresent or deceive.
health information	has the meaning provided in section 6 of the *Health Records and Information Privacy Act 2002* (NSW).
health privacy principles (HPPs)	means the principles set out in Schedule 1 to the *Health Records and Information Privacy Act 2002* (NSW).
information protection principles (IPPs)	mean the principles set out in Part 2 Division 1 of the *Privacy and Personal Information Protection Act 1998* (NSW).

eligible data breach	has the meaning given the *Data Breach Policy 2023* and s 59D of the *Privacy and Personal Information Protection Act 1998* (NSW). At the date of this policy this is: • unauthorised access to, or unauthorised disclosure of, personal information held by the University; which • a reasonable person would conclude would be likely to result in serious harm to an individual to whom the information relates. **Note**: Section 26WE of the *Privacy Act 1988* (Cth) has the same definition. See clause 13(5) of the *Data Breach Policy 2023* for when to notify the Commonwealth Information Commissioner.
personal information	has the meaning provided in section 4 of the *Privacy and Personal Information Protection Act 1998* (NSW).
privacy acts	means either or both of the *Privacy and Personal Information Protection Act 1998* (NSW) (the 'PPIP Act') and the *Health Records and Information Privacy Act 2002* (NSW) (the 'HRIP Act').
privacy management plan	means the privacy management plan required by section 33 of the *Privacy and Personal Information Protection Act 1998* (NSW) and established by clause 8 of this policy.
privacy officer	means the Manager, Archives and Records Management Services, or the occupant of any position nominated as privacy officer by the Chief Governance Officer.
unit	means, as appropriate, any of the following: • a faculty • University school • a portfolio controlled by a Deputy Vice-Chancellor, a Vice- President, the General Counsel or the Chief Governance Officer • a professional service unit within the portfolio of the Vice- President (Operations) • a Level 4 centre, as defined in the *Centres and Collaborative Networks Policy 2017*; and • other groups as determined by the Chief Governance Officer from time to time.

7 Privacy management principles

(1) The University, its staff, affiliates and, where appropriate, students must comply with all IPPs and HPPs.

(2) The IPPs and HPPs set out the legal requirements for:

(a) collecting personal and health information;

(b) storing personal and health information;

(c) access to and accuracy of personal and health information;

(d) using personal and health information; and

(e) disclosing personal and health information.

(3) In addition, HPPs set out further legal requirements for:

(a) using identifiers to protect identity;

(b) the right to anonymity in receiving health services;

(c) the flow of health information across the NSW border; and

(d) consent for linking health records of an individual in a system.

Note: See Part 2 Division 1 of the Privacy and Personal Information Protection Act 1998 (NSW); and Schedule 1 of the *Health Records and Information Privacy Act 2002* (NSW)

8 Privacy management plan

(1) The University's privacy management plan is set out in sub-clauses 8(1) to 8(6).

(2) This plan is:

(a) made in accordance with the University's policy framework established by clause 5 of the *University of Sydney (Policies Development and Review) Rule 2011* ; and

(b) supported by:

(i) this policy, which is publicly available on the University *Policy Register*;

(ii) the *Privacy Procedures 2023;* and

(iii) guidelines and information on the University's privacy website.

(3) The University will:

(a) provide a direct link to information about privacy (with a link to this policy) in the footer of the University's web site; and

(b) provide an online training course on privacy as part of its workplace ethics and integrity training program which all existing and new staff are required to complete.

Note: The online training course is available through Workday.

(4) A person who considers that the University has breached an IPP or HPP is entitled to an internal review of that conduct by the University.

(a) Applications for internal review must:

(i) be made in writing to a privacy officer by email or by mail at the address specified on the University's privacy website;

(ii) include a return address within Australia; and

(iii) be lodged within six months of the applicant becoming aware of the relevant conduct.

Note: The University's form for *Application for Review of Conduct under Section 53 of the PPIP Act* may be used for this purpose

(b) Upon receipt of an application for internal review, a privacy officer will:

(i) refer details of the application and the applicant's name to the NSW Privacy Commission, as required by section 54(1) of the PPIP Act; and

(ii) keep the NSW Privacy Commissioner informed of the progress of the review.

(c) The internal review will be decided by the Chief Governance Officer or, if that person is unable to do so, by the General Counsel.

(d) The decision maker will:

(i) come to a conclusion about the subject matter of the application;

(ii) advise the applicant of the results and of any action that the University proposes to take in respect of the complaint; and

(iii) report the findings and any proposed actions to the NSW Privacy Commissioner within 60 days of the date of receipt of the application.

(5) A person who is dissatisfied with the way the University deals with internal reviews or who disagrees with the University's findings can ask the NSW Civil and Administrative Tribunal (NCAT) to review the conduct.

Note: The address of NCAT is available on the University's privacy website.

(6) Whether or not a person applies for an internal review, they can also make a complaint to the NSW Privacy Commissioner about an alleged breach of their privacy.

Note: The address of the Commissioner is available on the University's privacy website.

(7) The University's privacy website will also provide:

(a) significant information about privacy, personal information and health information, and individual rights in relation to them;

(b) information, and links to relevant procedures, for staff, affiliates and students about collecting, storing, using and disclosing personal and health information;

(c) forms to apply for access to or amendment of personal or health information, and for making privacy complaints;

(d) contact details for the University's privacy officers.

(i) Privacy officers may be contacted on an identified or anonymous basis.

9 Eligible data breaches

(1) An eligible data 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.

(2) An eligible data breach 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.

(3) An eligible data breach requires high level coordinated management response from the University, which will be co-ordinated by the Manager, Archives and Record Management Services.

Note: See the *Data Breach Policy 2023* for the process to manage an eligible data breach involving personal or health information held by the University.

10 Tax file numbers

(1) As the recipient of tax file numbers, the University will collect, retain and disclose tax file number information of staff and students in accordance with taxation, personal assistance or superannuation law.

Note: See the *Privacy (Tax File Number) Rule 2015* issued under section 17 of the *Privacy Act 1998 (Cth)*

(2) Where required, the University will comply with the notifiable data breach scheme established by the *Privacy Act 1998 (Cth)*.

Note: See Schedule 1 the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*.

11 Roles and responsibilities

(1) **The Chief Governance Officer** is responsible for:

(a) determining applications for access to, and amendment of, personal information under the privacy acts; and

(b) determining applications for internal review conducted under Part 5 of PPIP Act;

(2) **The General Counsel** is responsible for making the decisions referred to in sub-clause 11(1) if the Chief Governance Officer is unable to do so.

(3) **The Manager, Archives and Records Management Services is responsible for**

(a) coordinating the management and reporting of eligible data breaches; and

(b) administering the University's compliance with the privacy acts

(4) **Privacy officers** are responsible for receiving:

(a) privacy complaints and requests for information access; and

(b) reports of breaches of the IPPs and HPPs.

(5) **Unit Heads** are responsible for:

(a) making contractors and consultants aware of their privacy obligations in relation to their engagement by the University; and

(b) requiring compliance with this policy and its associated procedures.

(6) **Staff, affiliates and, where appropriate, students:**

(a) are responsible for ensuring their own work practices comply with this policy and any associated procedures;

(b) must report any data breach to a privacy officer as soon as possible after becoming aware of it.

Note: ICT information security incidents must be reported to ICT Support using the Reporting a Cyber Security incident form

(7) **Staff and affiliates who direct students' research** are responsible for ensuring that students under their direction are informed of their obligations under the privacy acts.

12 Breaches of this policy

Failure to comply with this policy may constitute misconduct, and may result in disciplinary action being taken by the University.

13 Rescissions and replacements

This document replaces the following, which are rescinded as from the date of commencement of this document:

(1) Privacy Policy 2013, which commenced on 1 February 2013

(2) Privacy Management Plan 2013, which commenced on 4 April 2013

NOTES

Privacy Policy 2017

Date adopted:	15 December 2017
Date commenced:	24 April 2018
Date amended:	2 September 2021
	13 June 2023 (administrative amendments)
	20 December 2023 (administrative amendments)
Original administrator:	Group Secretary
Current policy owner:	Chief Governance Officer
Review date:	15 December 2022
Rescinded documents:	*Privacy Policy 2013*
	Privacy Management plan
Related documents:	*Privacy Act 1988 (Commonwealth)*
	Privacy and Personal Information Protection Act 1998 (NSW)
	Health Records and Information Privacy Act 2002 (NSW)
	Government Information (Public Access) Act 2009 (NSW)
	State Records Act 1998 (NSW)
	Data Breach Policy 2023
	Recordkeeping Policy 2017
	Research Data Management Policy 2014
	Recordkeeping Manual
	Advance Database Access Procedures 2013
	Research Data Management Procedures 2015

AMENDMENT HISTORY

Provision	Amendment	Commencing
8(4)(c); 11(1) and 11(2);	Reference to Group Secretary changed to General Counsel	2 September 2021
6	Replaced 'General Counsel' with 'Chief Governance Officer' Replaced 'Vice-Principal' with 'Vice-President' Replaced 'Director, University Libraries' with 'Chief Governance Officer' Replaced 'Vice-Principal (Operations)' with 'Vice-President (Operations)'	13 June 2023
6	updated link to *Centres and Collaborative Networks Policy 2017*	13 June 2023
8(4)(c); 11(1); 11(2); Notes	Replaced 'General Counsel' with 'Chief Governance Officer'	13 June 2023
8(2)(b)(ii)	updated link to *Privacy Procedures 2018*	13 June 2023
8(3)(b) note	replaced 'University's Careerpath website' with 'Workday'. Updated link	13 June 2023
8(4)(c); 11(2)	replaced 'Secretary to Senate' with 'General Counsel'	13 June 2023
11(6)(b) note	updated link to ICT Cyber Security reporting form	13 June 2023
6,9,11(3)(a)	replaced 'notifiable privacy breach' with 'eligible data breach' to reflect the amendments to the *Privacy and Personal Information Protection Act 1998 (NSW).*	20 December 2023
6,11(6)(b)	replaced 'privacy breach' with 'data breach' to reflect the amendments to the *Privacy and Personal Information Protection Act 1998 (NSW).*	20 December 2023
6	added definitions of 'data breach' and 'eligible data breach'.	20 December 2023