ACOM Privacy Policy

15 December 2017 v.2.2 (original October 2009)

1. Statement of intent

This policy:

a. states the College'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 College, its staff, students and affiliates; and

d. meets the statutory requirement for the preparation and implementation of a College privacy management plan.

2. Application

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

3. Definitions

privacy breach	means when personal or health information held by the College is: • lost; or • subjected to, or likely to be subjected to, unauthorised access, modification or disclosure.
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).
notifiable privacy breach	has the meaning given in clause 9 of this policy.
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 officer	means the Director of Ministry Services or such other person appointed by the Principal from time to time.

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.
unit	means, as appropriate, any of the following: • a faculty discipline • A College School, Institute or Centre • other groups as determined by the Principal from time to time.

4. Privacy management principles

a. The College, its staff, affiliates and, where appropriate, students must comply with all IPPsand HPPs.

b. The IPPs and HPPs set out the legal requirements for:

collecting personal and health information;

storing personal and health information;

access to and accuracy of personal and health information;

using personal and health information; and

disclosing personal and health information.

c. In addition, HPPs set out further legal requirements for:

using identifiers to protect identity;

the right to anonymity in receiving health services;

the flow of health information across the NSW border; and

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

d. The College will:

provide information about ACOM's privacy practice in the footer of the College web site.

e. A person who considers that the College has breached an IPP or HPP is entitled to an internal review of that conduct by the College.

f. Applications for internal review must:

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

include a return address within Australia; and

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

g. Upon receipt of an application for internal review, a privacy officer will:

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

keep the NSW Privacy Commissioner informed of the progress of the review.

h. The internal review will be decided by the Chair of the Academic Board or, if that person is unable to do so, by the Chair of the College Board

i. 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 College 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.

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

k. 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.

6. Notifiable privacy breaches

a. A notifiable privacy breach is a breach that requires notification to one or more of:

i. external stakeholders, such as the NSW Privacy Commissioner or the Commonwealth Privacy Commissioner; or

ii. internal stakeholders, such as those impacted by the breach and other College stakeholders.

b. A notifiable privacy breach involves one or more of:

i. a real risk of serious harm to those impacted by it;

ii. ongoing consequences, or the risk of ongoing consequences in terms of the number of people who may be impacted;

iii. the potential for serious reputational damage to the College; or

iv. the potential for legal or financial penalties to the College.

c. A notifiable privacy breach requires high level coordinated management response from the College, which will be co-ordinated by the Privacy Officer.

7. Tax file numbers

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

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

Where required, the College will comply with the notifiable data breach scheme established by the *Privacy Act 1998 (Cth)*. See Schedule 1 the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*.

8. Roles and responsibilities

The Privacy Officer is responsible for:

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

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

The Privacy Officer is responsible for

coordinating the management and reporting of notifiable privacy breaches; and

administering the College's compliance with the privacy acts

The Privacy Officer are responsible for receiving:

privacy complaints and requests for information access; and

reports of breaches of the IPPs and HPPs.

The Senior Team are responsible for:

making contractors and consultants aware of their privacy obligations in relation to their engagement by the College; and

requiring compliance with this policy and its associated procedures.

Staff, affiliates and, where appropriate, students:

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

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

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.

9. Breaches of this policy

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