

Privacy Policy

1. Purpose

UNSW College (the College) operates in complex regulatory and privacy compliance regimes established under both the federal and state legislative frameworks.

As a not-for-profit organisation with an annual turnover exceeding \$3 million, the College falls within the definition of an 'organisation' in the Privacy Act 1988 (Cth) and is required to comply with that Act as an "APP Entity". The College is also:

- (a) a "related body corporate" of UNSW Sydney as that term is defined by sections 46 and 50 (b) of the Corporations Act 2001 (Cth); and
- (b) a "controlled entity" of UNSW Sydney, as that term is defined by section 15A of the University of New South Wales Act 1989 (NSW); and
- (c) a "public sector agency" as that term is defined by section 3 (d) of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) and section 4 (d) of the Health Records and Information Privacy Act 2002 (NSW) (HRIPA).

As such, the College may be also required to comply with PPIPA and HRIPA.

UNSW may also collect data on citizens in European Union (EU) countries or process personal data of European residents and as such may need to comply with the European Union General Data Protection Regulation (GDPR).

The purpose of this Policy is to outline:

- (a) the Personal Information handling practices of the College;
- (b) the way individuals can access their Personal Information to seek the correction of it; and
- (c) how individuals may make a complaint to the College about the mishandling of their Personal Information.

2. Scope

This Policy applies to:

- (a) all College staff working for or on behalf of the College;
- (b) all College Students;
- (c) parents or guardians of the College Students who are under 18 years of age and School Students; and
- (d) third parties, such as customers, Business Partners and Service Providers of the College.

2.1 College Privacy Policy

The College is committed to only collect, hold, use and disclose Personal Information that is needed to carry out its functions and activities and to handle the information in accordance with the Privacy Laws and other applicable data protection laws.

It is College Policy to:

- (a) only collect Personal Information for a lawful purpose, which is directly related to the College's functions and activities;
- (b) not to collect Health Information or Sensitive Information from an individual unless the individual Consents to the collection of the information or unless the collection of the information is required or authorised by or under an Australian law;
- (c) only collect Personal Information directly from the individual concerned, unless the person has authorised collection from someone else, or where the person is under the age of 16, the information has been provided by a parent or guardian;
- (d) inform the person concerned that the College collects their Personal Information, the reason for collecting the information, how it is going to be used and disclosed (if applicable) and how the person can access and correct the information;
- (e) use all reasonable endeavours to ensure the collected information is relevant, accurate, complete, up to date and not excessive;
- (f) store Personal Information securely and protect it from unauthorised access, use modification or disclosure and destroy or de-activate the information if it is no longer needed;
- (g) provide access for individuals to their Personal Information and allow to update, correct or amend their Personal Information where necessary;
- (h) only use Personal Information for the purpose it was collected unless the person has given their Consent or if exemptions apply;
- (i) only disclose Personal Information with a person's Consent or if exemptions apply.

3. Policy statement

3.1 College functions

The College operates in educational areas that are ancillary to the core business (research and degrees) of UNSW Sydney. The College's core function is education though this is supported by a number of functions including IT, finance, human resources, legal and compliance, sales and marketing.

3.2 Collecting Personal Information

- (a) The College may collect the following information:
 - i. Personal Information, such as: the individual's name, date of birth, contact details, including postal and residential address, email address, phone number and/or mobile number (see Annexure 1 for further examples);
 - ii. Sensitive Information, such as: racial or ethnic origin or criminal record;
 - iii. Health Information, such as: information or opinion about the health or a disability of an individual, e.g. professional medical practitioner certificates.
- (b) The College may collect Personal Information, Sensitive Information and Health Information in a number of ways, including the following:

- i. Directly from individuals or their authorised representative, for example when the individuals: complete online or hardcopy forms; submit assessment materials, applications, instructions or invoices; speak with College staff in person or by telephone; correspond with the College by letter or email; use the College websites or social media platforms; or participate in the College's marketing initiatives;
 - ii. Indirectly from Education Agents and Service Providers where an individual gave Consent for the information to be collected and disclosed to the College, or as otherwise legally permitted by applicable Privacy Law;
 - iii. Automatically through digital communication information from search engines or the College website hosts (including through the use of cookies and similar technology). This information includes the individual's Internet Protocol (IP) address and the web pages visited immediately before and after accessing UNSW website.
- (c) The College may collect Personal Information for primary and secondary purposes:

Primary Purposes:

- i. Delivery of education services including, but not limited to: recruitment, admission, teaching, assessments, academic administration, research, market research, and analysis of data which includes de-identified Personal Information of College Students or prospective students.
- ii. Interactions with UNSW Sydney as the College's parent entity, for example, for the purpose of managing emergencies; facilitating access by College Students to UNSW Sydney services and support, either in their capacity as College Students or when transitioning to UNSW Sydney to commence studies at UNSW Sydney; collaborating with UNSW Sydney for commercial purposes, including but not limited to conducting tests and research; reporting to UNSW Sydney as a controlled entity and as an entity that delivers educational services under UNSW Sydney's CRICOS code.
- iii. Conducting its business operations including, but not limited to: dealing with requests, enquiries or complaints from College Students, School Students and their parents or guardians; facilitating fee payments and refunds; dealing with the College's customers, Business Partners and Service Providers, and other third parties, such as banks and financial service providers; for human resources purposes (including health and safety risk management); or for interacting with other organisations and companies.

Secondary Purposes:

- i. Showcasing achievements of College Students and School Students, for example, in student graduation books or year books, testimonials, in-house videos or Student Newsletters.



- ii. Marketing, advertising and promoting College products and services for example, in marketing materials, testimonials, via the College website and through social media.
- iii. College informs individuals that it collects their Personal Information, either at or before the time of collection, or as soon as practicable thereafter, either through a form used to collect the information or by giving a notice to individuals or by otherwise ensuring that the individuals are aware of the collection of their Personal Information. The notification will be in writing wherever possible.
- iv. Further examples of College's functions and activities and the type of Personal Information collected are outlined in Annexure 1.

3.3 Consent

Where necessary and as required by law, the College may seek specific Consents from an individual to collect, use and disclose the individual's information.

Consent must be sought when:

- (a) the College collects Sensitive Information about an individual, unless the collection of the information is required or authorised by or under an Australian law or a court/tribunal order;
- (b) the use or disclosure of Personal Information is not directly related to the primary purpose of collection, unless:
 - i. the individual would reasonably expect the College to use or disclose the information for the secondary purpose or the use; or
 - ii. the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;
- (c) the College collects and uses Personal Information, such as testimonials or photos of an individual in marketing or advertising materials. Note, Consent is only required where the person's identity is clear or can reasonably be ascertained from an image or a video, and in case of testimonials, where the testimonial contains personally identifiable information. College staff may obtain copies of the Student Consent Form and the Parent/Guardian Consent Form as relevant to their activities by visiting the Forms page on the College website or College intranet;
- (d) the use or disclosure of Personal Information is for the purpose of Direct Marketing, unless certain exceptions under the law apply;
- (e) the College discloses Personal Information about an individual to an Overseas Recipient, unless:
 - i. the Overseas Recipient of the information is subject to a law that has the effect of protecting the information similar to the Australian Privacy Principles; and
 - ii. there are mechanisms that the individual can access to take action to enforce that protection of the law; or the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

- iii. the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or
- iv. the College reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, and the Overseas Recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

3.4 Consent is not required

Consent is not required if there is a Permitted General Situation, for example, the College reasonably believes that the collection, use or disclosure is necessary:

- (a) to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
- (b) where the College has reason to suspect that unlawful activity, or misconduct of a serious nature that relates to College's functions or activities has been, is being or may be engaged in, and the collection, use or disclosure is necessary in order for the College to take appropriate action in relation to the matter; or
- (c) where the College reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP Entity, body or person to locate a person who has been reported as missing.

3.5 Anonymity and pseudonymity

- (a) For most of its functions and activities, the College needs Personal Information from identifiable individuals to perform its operations, e.g. to deliver educational services, to conduct educational assessments, or to handle an inquiry or complaint etc.
- (b) Where practicable, an individual can choose not to identify themselves or to use a pseudonym. For example, if an individual calls the College to make a simple enquiry, they will not be asked about their name and contact details unless this information is needed to provide a response.

3.6 Storage, security and disposal

- (a) Where practicable, the College will seek to ensure that Personal Information is stored securely within Australia.
- (b) Where the College engages Service Providers to store Personal Information, the College will seek assurance in its contracts with the Service Providers that they will comply with applicable privacy and data protection law.
- (c) The College has processes in place to limit access to Personal Information and to prevent unauthorised access, by using measures, such as: user identification, the encryption of data or different level of user access.
- (d) College staff are permitted to email or otherwise transfer Personal Information held on College's systems to outside systems (such as their personal email accounts or file hosting services) only if it is absolutely necessary, i.e., for a justified

academic, research or business need, and if it is done in accordance with the College [IT Security Policy](#), [Bring Your Own Device Policy](#) and relevant procedures.

- (e) The College will securely destroy or de-identify Personal Information it holds once the Personal Information is no longer needed for any purpose for which the information was collected. This requirement does not apply where the Personal Information is contained in a Commonwealth or state record (for the purposes of records retention laws) or where the College is otherwise required by law to retain the information.

3.7 Direct Marketing

- (a) The College may use Personal Information collected directly from an individual for the purpose of Direct Marketing, provided that individual has opted in to receive such communications.
- (b) An individual can request not to receive Direct Marketing communications from the College by opting out of receiving future emails or SMSs.
- (c) The College provides information about how to opt out in each Direct Marketing communication.

3.8 Disclosing Personal Information

- (a) The College is a related body corporate and a controlled entity of UNSW Sydney. Section 13B of the Privacy Act 1988 (Cth) permits UNSW College to disclose Personal Information to UNSW Sydney as is necessary to carry out its activities and functions, including those set out in paragraphs 3.1, 3.2 and Annexure 1 of this Policy.
- (b) The College may disclose Personal Information to other third parties in the following cases:
 - i. to College's agents, consultants, contractors and Service Providers who assist UNSW College in running its business or provide related services, and who are subject to security and confidentiality obligations;
 - ii. to UNSW College Business Partners, to the extent they are involved in the provision of UNSW College services to customers;
 - iii. where an individual has consented the disclosure to a third party; or
 - iv. if the law allows or requires UNSW College to do so.
- (c) UNSW College will not disclose Sensitive Information without obtaining the Consent of the individual unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person or in accordance with section 16A of the Privacy Act 1988 (Cth).
- (d) While the College's main teaching venues are in New South Wales, it operates in more than 20 countries worldwide, predominantly in the Asia-Pacific region. The College may disclose Personal Information, outside New South Wales, to Commonwealth government agencies or to Overseas Recipients where:
 - i. the College has taken reasonable steps to ensure the Overseas Recipient does not breach the Privacy Principles in relation to the information; or

- ii. the College reasonably believes that the Overseas Recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information, and there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- iii. the individual has expressly consented for the College to do so; or
- iv. as set out in section 3.4 of this Policy.

3.9 Privacy Impact Assessment

When developing or reviewing a project, such as: new or amended programs, activities or databases, the College may consider the need for a Privacy Impact Assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy, and makes recommendations for managing, minimising or eliminating privacy impacts.

3.10 Notifiable Data Breach

In the case of an Eligible Data Breach, the College will inform the OAIC and IPC and affected individuals in the manner required by the Privacy Act 1988 (Cth) and the PPIPA.

3.11 The General Data Protection Regulation (GDPR)

The GDPR and the Privacy Act 1988 (Cth) share many common requirements, however, there are also some notable differences. Where the College is engaging in business in the European Union that is likely to result in data being collected or processed in relation to European residents, the Legal and Compliance team needs to be consulted, who can advise on the nature of responsibilities that the College may have under the GDPR, before commencement of activities.

3.12 Accessing and correcting Personal Information

Accessing Personal Information

An individual (including a UNSW College Student or School Student) may request access to Personal Information which the College holds about them by sending a written request to the attention of the UNSW College Privacy Officer:

- By email: legalandcompliance@unswcollege.edu.au
- By post: Legal and Compliance Team
UNSW Global Pty Limited
223 Anzac Parade
Kensington NSW 2033

The College will consider the individual's request for access and may request the individual to verify their identity. There may be limited circumstances where the College is unable to provide the individual with access to the information, such as if giving access would be unlawful, would have an unreasonable impact on the privacy of other individuals, or for other reasons set out in the Privacy Laws. The College will otherwise provide the individual with access to the Personal Information in the manner requested by the individual (if it is reasonable and practicable to do so), or otherwise in a way that meets the needs of UNSW College and the individual, within a reasonable period after



the request is made (generally within 30 days). If the College refuses to give access to the Personal Information, or to give access in the manner requested by the individual, the College will provide the individual with written reasons for the refusal and the mechanisms available to the individual to complain about the refusal.

There is no fee for making a request to access the information. Generally, the College will not charge a fee for providing access to the information to the individual, unless it requires a significant amount of time to locate the information or to collate the information or present the information in an appropriate form.

Correcting Personal Information

If an individual (including a UNSW College Student or School Student) believes that the Personal Information which the College holds about them is inaccurate, out-of-date, incomplete, irrelevant or misleading they have the right to request the information to be corrected.

To request amendment of his/her Personal Information, the individual should:

- (a) Provide his/her personal and contact details, and describe the Personal Information about him/her that they would like to amend, providing the reasons that he/she considers the information to be incomplete, incorrect, out-of-date, or misleading;
- (b) Send the request to the attention of the UNSW College Privacy Officer:
 - By email: legalandcompliance@unswcollege.edu.au
 - By post: Legal and Compliance Team
UNSW Global Pty Limited
223 Anzac Parade
Kensington NSW 2033
- (c) To prevent adverse consequences of unauthorised disclosure of Personal Information, the College will verify the individual's identity and authority to request the change prior to processing the request.
- (d) There is no fee to request correction of Personal Information.
- (e) The College will aim to respond to the request within 30 days.

3.13 Complaints about handling Personal Information

If an individual believes that the College has misused their Personal Information, they can contact the College Privacy Officer to discuss and try to resolve the issue informally or lodge an application for a formal review with the College, or complain to the OAIC.

Please note that the OAIC generally requires individuals to complain directly to the agency or organisation (in this case, the College) and allow thirty (30) days for it to respond before the individual can lodge a complaint with the OAIC.

To lodge an application for a formal review with the College, an individual should:

- (a) Complete a Complaint Form in line with the College Student Grievances and Complaints Policy within twelve (12) months of the time an individual became

aware of the misuse of their Personal Information. The Complaint Form is available at Annexure 2 of this Policy.

- (b) The complaint can be made about:
 - i. Collection of Personal Information;
 - ii. Security or storage of Personal Information;
 - iii. Refusal to access or find out about Personal Information;
 - iv. Accuracy of Personal Information;
 - v. Use of Personal Information; and
 - vi. Disclosure of Personal Information.
- (c) Email or post the Form to the College Privacy Officer.
- (d) The individual will be informed in writing of the result of the review.
- (e) The College aims to respond to the complaint within ten (10) working days. If the complaint is complex and requires more extensive investigation, the College will use all reasonable endeavours to complete the review within thirty (30) days.
- (f) If the individual is unhappy with the result of the review, he/she can lodge a complaint with the OAIC. Information on how to lodge a complaint can be found on the [OAIC website](#).

4. Roles, responsibilities, and delegations

Role	Responsibility
Head of Legal, Risk and Compliance	Implementing, disseminating and reviewing this Policy.
Legal Counsel	The day to day implementation of this Policy and being the first point of contact for all enquiries that relate to this Policy.

5. Definitions

Definitions and Acronyms	
Australian Privacy Principles (APPs)	means the 13 Privacy Principles set out in Schedule 1 of the Privacy Act 1988 (Cth) which outline how APP entities must handle, use and manage Personal Information.
APP Entity	means an agency or an organisation, including all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health Service Providers and some small businesses.
Business Partner	means a person who is part of a business partnership, collaboration or similar arrangement with UNSW College.

Consent	Consent means 'express consent or implied consent'. The four key elements of consent are: (a) the individual is adequately informed before giving consent (b) the individual gives consent voluntarily (c) the consent is current and specific, and (d) the individual has the capacity to understand and communicate their consent.
CRICOS Code	means the Australian Commonwealth Register of Institutions and Courses for Overseas Students.
Direct Marketing	means the use and/or disclosure of Personal Information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising.
Education Agent	A person or organisation (in or outside Australia) who recruits overseas students and refers them to education providers. Education agents may provide education counselling to overseas students as well as marketing and promotional services for education providers.
Express Consent	means Consent given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.
Eligible Data Breach	means a data breach where: (a) both of the following conditions are satisfied: i. there is unauthorised access to, or unauthorised disclosure of, the information; ii. a reasonable person would conclude that the access or disclosure would be likely to result in Serious Harm to any of the individuals to whom the information relates; or (b) the information is lost in circumstances where: i. unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and ii. assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in Serious Harm to any of the individuals to whom the information relates.
GDPR (General Data Protection Regulation)	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and enforced as of 25 May 2018, as amended, replaced or superseded from time to time.

Health Information	Health Information as defined by the Privacy Act 1988 (Cth) means: (a) information or an opinion about: i. the health or a disability (at any time) of an individual; or ii. an individual's expressed wishes about the future provision of health services to him or her; or iii. a health service provided, or to be provided, to an individual; that is also Personal Information; or (b) other Personal Information collected to provide, or in providing, a health service; or (c) other Personal Information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.
HRIPA	means the Health Records and Information Privacy Act 2002 (NSW)
Information Protection Principles (IPPs)	means the 12 Principles set out in Part 2, Division 1 of the PPIPA outlining legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information.
Implied Consent	arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.
IPC	Information and Privacy Commission NSW (who oversees the PPIPA)
Notifiable Data Breach	means a scheme that requires agencies and organisations to notify individuals whose personal information is involved in a data breach that is likely to result in Serious Harm and to notify Australian Information Commissioner of Eligible Data Breaches.
OAIC	means the Office of the Australian Information Commissioner (who oversees the Privacy Act 1988 (Cth)).
Overseas Recipients	means a person or entity who is not in Australia or an external Territory, and is not the entity or the individual, and includes UNSW College staff in UNSW College's subsidiary companies located overseas and Education Agents.
Permitted General Situation	has the meaning in section 16A of the Privacy Act 1988 (Cth).
Personal Information	Personal Information as defined by the Privacy Act 1988 (Cth) means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

	(a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not. Examples of Personal Information include: (a) a record which includes an individual's name, address, date of birth, mobile phone number, email address; (b) photographs, images, video or audio footage of an individual; (c) the fingerprints, blood or DNA samples of an individual.
PPIPA	means the Privacy and Personal Information Protection Act 1998 (NSW).
Privacy Laws	means the Privacy Act 1988 (Cth), PPIPA and HRIPA.
Privacy Principles	means Australian Privacy Principles and/or Information Protection Principles
School Student	means a person formally engaged in learning, usually one enrolled in a primary or secondary school.
Sensitive Information	Sensitive Information is defined in s.6 of the Privacy Act 1988 (Cth) to mean: (a) information or an opinion about an individual's: i. racial or ethnic origin; or ii. political opinions; or iii. membership of a political association; or iv. religious beliefs or affiliations; or v. philosophical beliefs; or vi. membership of a professional or trade association; or vii. membership of a trade union; or viii. sexual orientation or practices; or ix. criminal record; x. that is also Personal Information; or (b) Health Information about an individual; or (c) genetic information about an individual that is not otherwise Health Information; or (d) biometric information that is to be used for the purpose of automated biometric (e) verification or biometric identification; or (f) biometric templates.
Serious Harm	means serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.

Service Provider	means a third party that provides services on behalf of UNSW College to UNSW College Students and/ or staff under a written agreement.
UNSW College Student	means a student who is enrolled with UNSW College or a person who has submitted an application for admission to UNSW College.
UNSW Sydney	means the University of New South Wales (ABN 57 195 873 179).

Related Policy Documents and Supporting Documents	
Legislation	- Privacy Act 1988 (Cth) - Privacy and Personal Information Protection Act 1998 (NSW) - Health Records and Information Privacy Act 2002 (NSW) - Corporations Act 2001 (Cth) - University of New South Wales Act 1989 (NSW) - European Union <i>General Data Protection Regulation</i> (2016/679)
Policy & Procedures	- Data Breach Policy and Procedure Data Governance Policy IT Security Policy - Data Classification Standard

6. Policy Governance

Privacy Policy	
Category/Business Group	Legal and Compliance
Published Externally (Yes/No)	Yes
Approver	Chief Executive Officer
Responsible Officer	Chief of Staff
Contact Officer	Head of Legal, Risk and Compliance
Effective Date	24/02/2024
Next Review Date	24/02/2027
Version	2.0

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
2.0	Sarah Lightfoot - Chief Executive Officer	24/02/2024	24/02/2024	- Definitions section replaced. - Section 3.2 split into sub-list of 3.2.1, 3.2.2

				and 3.2.3 for ease of reference and understanding. ▪ Correction to referencing at paragraph 3.8. ▪ Corrections to list/sub-list formatting throughout document. ▪ References to 'UNSW College' replaced with 'the College' where appropriate. ▪ Corrections of typos in the policy. ▪ Additions to section 3.12 to include an individual's access to information held by College.
1	Sarah Lightfoot - Chief Executive Officer	11 August 2023	17 August 2023	N/A

Please visit our website to ensure that you have the latest version of this Policy. Policies are available at: unswcollege.edu.au/about/policies

Annexure 1

Business Group	Functions and Activities	Type of Personal Information Collected
Academic, Student Administration/Services and Recruitment		
<i>Academic, Student Administration / Services and Recruitment</i>	Delivering English language programs and university pathway programs to UNSW Sydney and other universities International student recruitment, admissions, academic administration and student services <i>Examples of activities:</i> - receiving and considering Student applications - where UNSW College Students have applied through an Australian or overseas Education Agent, sharing information about the UNSW College Student with the Education Agent - administering grievances, complaints and appeals processes - administering disciplinary processes - providing administrative services for a wide range of matters including UNSW College Student enrolment, progress and welfare - responding to queries (whether online, over the phone or in person) - managing adjustments for UNSW College Students with a disability - assisting when UNSW College Students ask for help on personal issues (eg referrals to counsellors, liaising with	<i>Examples: UNSW College Students</i> - name - physical address - mobile phone number - landline - social media contact details - student and personal email addresses - date of birth - gender - citizenship - passport number - student visa - academic records and transcripts - enrolment details - student number - Unique Student Identifier (for domestic students in certain English courses) - assessment results - records relating to complaints, appeals, grievance procedures or misconduct - photographs, videos or other recordings that identify the UNSW College Student - if a parent or guardian, their relationship to the UNSW College Student - health and other Sensitive Information where this affects a

Business Group	Functions and Activities	Type of Personal Information Collected
	doctors and other specialists and UNSW Sydney) ▪ providing recreational activities, support services and social events for UNSW College Students, such as excursions, graduation ceremonies, year books, ▪ assisting UNSW College Students who transition to UNSW Sydney after completing their studies with UNSW College ▪ dealing with third parties that provide goods or services to UNSW College Students where we have been involved in procuring the good or service for the student (eg health insurance providers) ▪ communicating with UNSW College Students about matters related to their study ▪ to confirm a student's identity at assessments ▪ marketing UNSW College's services through all forms of media (including our website, social media pages, brochures and pamphlets) ▪ conducting research and analysis (including market research) ▪ managing emergencies ▪ communicating with UNSW College Students about emergencies identified by UNSW Sydney	UNSW College Student's progress or assessment, the management of emergencies or other aspects of a person's welfare ▪ in the context of a complaint, Personal Information about the complainant and others who are involved, in order to deal with the complaint ▪ in the context of disciplinary or misconduct proceedings, Personal Information about the UNSW College Student in question and others who are involved, in order to deal with the matter

Business Group	Functions and Activities	Type of Personal Information Collected
Other UNSW College Business Groups		
<i>Other UNSW College Business Groups perform business support functions such as Human Resources, Finance, IT, Marketing and Legal and Compliance. These Business Groups support UNSW College's core activities.</i>	Human Resources - recruiting new staff - maintaining staff records - managing staff performance management, complaints, misconduct and grievance procedures - managing adjustments for staff with a disability or health condition as applicable - assisting where staff ask for help with personal issues - staff health and safety risk management	<i>Examples of types of Personal Information about staff or applicants</i> - name - residential address - mobile phone number - landline - personal email addresses - work email address - date of birth - gender - employment history - qualifications, education and training - academic transcripts - employer references - criminal history (where relevant to position) - Working with Children Check (where relevant to position) - in the context of a complaint, Personal Information about the complainant and others who are involved, in order to deal with the complaint - Health Information - in the context of disciplinary or misconduct proceedings, Personal Information about the staff in question and others who are involved, in order to deal with the matter
	Finance and Facilities	<i>Examples of types of Personal Information</i>

Business Group	Functions and Activities	Type of Personal Information Collected
	- managing UNSW College Student fees and payment matters - managing staff payroll and benefits - managing staff use of corporate credit cards - workspace resource management (such as desk and meeting room bookings)	- information in relation to staff salaries and benefits - Payee identity checks for refunds - staff bank account information - work location (as updated from time to time across authorised worksites)
	<i>IT</i> - managing the access controls, security and integrity of data held in College's information systems, including - databases (e.g. UNSW College Student information databases managed by College's Admissions team and employee data managed by our HR team) - content management systems (such as our contracts management system) - outsourcing IT functions to third parties (such as cloud service providers) where such parties are subject to confidentiality and security obligations - managing data back-up processes	<i>Examples of types of Personal Information about staff, visitors, and UNSW College Students</i> IT has a role in supporting all College's systems which contain Personal Information. Examples of Personal Information which IT handles in a more direct way include: - usernames and passwords - email addresses - IP addresses - use and consumption of UNSW College's developed or procured IT products and services (e.g. websites, business software and digital devices).
	<i>Marketing</i> preparing, publishing or distributing advertising, promotional and other marketing material (e.g. on our website, social media pages, hard copy brochures,	<i>Examples of types of Personal Information about UNSW College Students, staff and School Students</i> - name - physical address

Business Group	Functions and Activities	Type of Personal Information Collected
	handbooks and pamphlets, video testimonials) ▪ running recruitment and promotional events (e.g. at careers fairs) ▪ running trade promotions ▪ communicating with UNSW College Students or potential UNSW College Students for marketing purposes (including by email or mobile phone where UNSW College Students have opted in to receive such communications, but we will always provide a straightforward way of opting out) ▪ collecting data, conducting research and performing analysis to improve existing, and develop new, products and services	▪ mobile phone number ▪ landline ▪ social media contact details ▪ UNSW College Student and School Student and personal email addresses ▪ date of birth ▪ job title (if a staff) ▪ student number (if a UNSW College Student) ▪ photographs, videos or other recordings that identify the UNSW College Student, staff or School Student (though we will seek specific Consent unless it is not reasonably practicable to do so)
	<i>Legal and compliance</i> Advising UNSW College on the following: ▪ its legal rights and obligations in relation to UNSW College Students or School Students; parents or guardians of Under 18 UNSW College Students or School Students; staff; and third parties such as customers, Business Partners and others ▪ regulatory compliance matters ▪ student complaints, misconduct or disciplinary matters ▪ staff complaints, misconduct or disciplinary matters	All the types of Personal Information we hold, including the examples in this table.

Business Group	Functions and Activities	Type of Personal Information Collected
	- negotiating and managing contracts - litigation and disputes to which it is a party - briefing external solicitors, barristers and other advisers - agreements and arrangements with UNSW	
All UNSW College Business Groups		
<i>All Business Groups</i>	Engaging third party suppliers (e.g. cloud service providers, IT providers and consultants) to enable UNSW College to improve its infrastructure, systems, processes, products and services	All the types of Personal Information we hold, including the examples in this table.
	All interactions with UNSW Sydney as UNSW College's parent entity, including: - administering packaged offers of admission to UNSW College and UNSW Sydney - managing emergencies (including calling or texting UNSW College Students and UNSW College staff on their mobile or other devices); - facilitating access by UNSW College Students to UNSW Sydney services such as UNSW Sydney Disability Services, counselling and health services - complaints, disciplinary and misconduct matters affecting UNSW College or UNSW Sydney - working with UNSW Sydney to improve existing, and develop new, products and services to UNSW College Students or	All the types of Personal Information we hold, including the examples in this table.



Business Group	Functions and Activities	Type of Personal Information Collected
	UNSW Sydney students (which may involve collecting and sharing data with UNSW Sydney, and performing research and analysis) ▪ maintaining and developing UNSW Sydney and UNSW College's business infrastructure, services, systems and processes.	
	▪ Exercising our rights, or fulfilling our obligations under, a contract with an individual. ▪ Communicating with customers in order to improve our services. ▪ Sending information and material that are related to UNSW College services or that may be of interest to a customer. Any other purpose for which Personal Information was provided to UNSW College or for any purpose related or ancillary to any of the above.	All the types of Personal Information we hold, including the examples in this table.



Annexure 2 - Complaint Form

Full Name			
Postal Address			
Phone Number			
Email Address			
Please tick which of the following describes your complaint: <i>(you may tick more than one option)</i>: ☐ collection of my Personal, Sensitive or Health Information ☐ security or storage of my Personal, Sensitive or Health Information ☐ refusal to let me access or find out about my own Personal, Sensitive or Health Information ☐ accuracy of my Personal, Sensitive or Health Information ☐ use of my Personal, Sensitive or Health Information ☐ disclosure of my Personal, Sensitive or Health Information ☐ other <i>(please specify)</i>:			
Please describe the details of your complaint and dates where relevant			
Attached documents	☐ I am attaching supporting documents ☐ I am not attaching supporting documents		
Signature		Date	

Office Use Only

Received by		Date	
Signature		Date	