EXCELSIA COLLEGE
Sydney

INFORMATION MANAGEMENT AND PRIVACY FRAMEWORK

GOV-STA-04

Objects of Excelsia College

Motivated by the Christian faith, as expressed by the Apostles' Creed and Nicene Creed, with fidelity to the Scriptures as the Word of God, the objects of the College are the advancement of the Christian faith and higher education.

1 Policy statement and principles

Excelsia College is committed to the collection, storage and safeguarding of personal information and vital and important records in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles. This policy framework describes the ways in which the College deals with personal information. The purpose of this policy framework is to:

- ensure that any personal information and personal data collected from students and employees will be used by the College in accordance with and as described in this policy framework
- provide guidance and standards for the storage of institutional documents and records, and for access that protects the rights and interests of the organisation and its students and staff.

1.1 Collection of personal information

i. The College will only collect personal information about an individual that is needed for the College to offer higher education services, including what is needed to comply with necessary government, legislative or accrediting authorities. The College collects information necessary to enable the College to:

   a. provide services to students and to people enquiring about study at the College
   b. process applications for admission
   c. communicate with students
   d. maintain appropriate academic and financial records
   e. perform other internal administrative functions
   f. maintain contact with alumni
   g. provide statistical and other information required by the government.

ii. Student personal information collected and stored by the College may include information to enable the College to identify a student and communicate with the student or graduate; information relating to the student's educational background, qualification and academic results; outcomes of grievances and misconduct; banking and payment details; visa information; the student's Unique Student Identifier (USI); information regarding a graduate's employment.

iii. Employee or contractor information collected and stored by the College may include personal information relating to identity; employment history and qualifications; business; and any other information that may be legitimately requested to facilitate employment or engagement.

iv. The College will normally inform the individual if it is collecting information about them, why it needs to do this, and to whom the College provides that information.

v. The collection of personal information will occur through approved forms. Such forms will seek specific information required for the purpose of conducting higher education courses and related activities.

vi. The College will do its best to ensure the information collected is relevant, up to date and complete.

1.2 Storage, use and handling

1.2.1 Personal information

i. The College will only use an individual's personal information for the purpose(s) for which it was collected and for other secondary purposes directly related to that primary purpose, unless the individual consents to another use, the use is necessary to protect that individual against serious threat, or the use is required by law.

ii. The College retains student information provided to it and which it collects, including personal information and personal data in accordance with legislative requirements and College procedures for storage and handling of records. For student information, this is generally so long as the College continues to provide services to that student and for seven years after that student leaves the College.

iii. The College retains information relating to Working With Children Checks and police checks for the duration of that individual's engagement with the College and for a minimum of seven years after the individual ceases their engagement with the College.

iv. The College will maintain a statement of the types of personal information it holds and why it is held, how long it is kept for, who can access it, and how people should go about getting access to it.

v. The College will take reasonable care to check that an individual's information is accurate, up to date and complete, before using it.

vi. The College will protect an individual's information against any form of misuse, and prevent unauthorised use or disclosure.

vii. The College will only update and amend records of personal information when the individual concerned requests such amendment.

viii. Any intended use of sensitive information on the basis to lessen or prevent a serious threat should be made through a formal request includes:

a. substantive evidence provided to allow an assessment of the specific threat

b. outline of the information to be released including:

- information to be released
- authorised recipients of the information (internal or external).

c. intended use of the information.

1.2.2 Records and documentation

i. Excelsia College is committed to managing, controlling and disposing of its records and documents in line with relevant legislation and best practice.

ii. Each staff member of the College is responsible for maintaining accurate student and alumni records that relate to their School or Department.

iii. Vital records are stored digitally and are held and/or backed up daily offsite. Digital access is managed through security permissions..

iv. Important records are stored digitally wherever possible, with securities similar to those for vital records. Hard copy files are held in secured filing cabinets in physical locations that are maintained and protected in the best manner possible.

v. Staff and student research data is collected, stored and secured in accordance with the Research Framework.

1.3 Disclosure of personal information

i. The College does not disclose personal information to third parties without the owner's explicit consent, unless required or permitted by law.

ii. The College will endeavour to ensure that the recipient only use or disclose an individual's personal information for the purpose for which it was given.

iii. Where the College transfers or discloses personal information to third parties, including to persons or businesses outside Australia, the College enters into binding contractual arrangements with such third parties and takes reasonable steps to ensure that:

   a. the recipients of such information do not breach the Australian Privacy Principles (and where appropriate the General Data Protection Regulation, GDPR) in relation to that information

   b. personal information is used only as part of the primary purpose for which it was provided (or for any secondary purposes directly related to that primary purpose).

iv. The College is required by law to inform the relevant Australian government department if an overseas student visa holder:

   a. changes the course of study for which they are enrolled

   b. changes the duration of their course of study

   c. breaches a student visa condition relating to attendance or satisfactory academic performance.

v. Personal information may be disclosed for the prevention, detection or investigation of criminal or proscribed conduct, or in certain circumstances in the interest of public health or public safety.

vi. It may sometimes be necessary for the College to provide personal information to others with whom it conducts business, e.g. insurers, companies developing and providing educational software systems.

1.4 Access to personal information

i. The College will give individuals access to their personal information as held by the College, subject to restrictions in other government legislation.

ii. If a student wishes to gain access to their personal information held by Excelsia College, they should complete the Student Request for Access to Own Personal Information form.

iii. If a staff member wishes to gain access to their personal information or employee records held by Excelsia College, they should contact People and Culture to request this access. It should be noted that the *Privacy Act 1988* (Cth) does not apply to the use or disclosure of any employee records held by a private-sector employer if these actions directly relate to the current or former employment relationship.

iv. If a graduate of the College wishes to gain access to their personal information held by Excelsia College, they should contact the Registrar's Office.

v. An individual can request amendment to their personal information if they believe that it is inaccurate, out of date, incomplete, irrelevant, or misleading. Students should submit a Change of Personal Details form to update their personal information.

1.5 Complaints about privacy and the handling of personal information

i. Any person may make a complaint to the College regarding its dealings with personal information including any breaches of the College of any Australian Privacy Principles.

ii. If a person has any complaints about the College's dealings with their personal information including any breaches by the College of any Australian Privacy Principles or any questions regarding this policy framework, they are able to submit that complaint or query by contacting the College at info@excelsia.edu.au.

iii. Any complaints about privacy received by the College will be referred to the Chief Executive for prompt investigation and a written response will be provided to the complainant as soon as possible.

iv. The College takes complaints seriously and aims to resolve them quickly and fairly. Should the complainant not be satisfied with the resolution of any privacy complaints, they are able to seek further redress through the Office of the Australian Information Commissioner or the Health Complaints Commission.

1.6 Website data

i. The College stores personal information electronically and in hard copy form. Personal information kept in electronic databases is protected by the College's Information and Communication Technology security. All financial transactions processed by the College and the use of payment details meet industry standards.

ii. When accessing the College's website, log files are created by the web server, showing the IP address of the visitor, time, date, and pages visited. The information generated in web logs may be used to generate statistics about access to the College site. In certain restricted areas (online areas where login is necessary), the website uses cookies, which are text files placed on computers. These cookies help the website analyse how users use the site. This information will

only be used for statistical purposes but will be transmitted to and stored by Google on servers in the United States. Visitors may refuse to use cookies by selecting the appropriate settings on their browser, but this may limit use of the website. By using the website in those limited areas, visitors consent to the processing of data about them by Google for the limited purpose above.

iii. The College may use web beacons and QR codes to track the visiting patterns of individuals accessing its website.

iv. While the College has secure password protections in place for the College's website, there is always a possibility that any personal information disclosed online may not be fully protected. Individuals disclosing personal information online should ensure they remain vigilant when using their College accounts and avoid disclosing their passwords or login details to third parties.

v. If an individual becomes aware of a security issue or has concerns about any information they may have disclosed on the website, they should contact the College's Information Technology service desk as soon as possible.

Non-compliance with this policy framework may result in disciplinary action in accordance with Excelsia College by-laws.

2 Scope

This policy framework applies to all College staff and students, prospective students, and graduates of the College.

3 Roles and responsibilities

The following stakeholders have a responsibility in relation to this policy framework.

Role	Responsibility
Chief Academic Officer	• the safe storage and handling of student assignments and other assessed works • the safe storage and handling of course details
Chief Executive	• managing any complaints about privacy and ensuring a written response is provided to the complainant as soon as possible • the safe storage and handling of contracts, deeds, insurance policies • the safe storage and handling of proof of provider accreditation, registration, certification, etc. • monitoring the effectiveness of this framework within their scope of responsibility • making recommendations with respect to this framework to appropriate personnel and committees
Chief Financial Officer	• undertaking risk management processes in relation to information and records, report to Management Committee, and take steps to minimise hazards identified

Chief Strategy Officer and Director of Quality	• the safe storage and handling of proof of course accreditation, registration, certification, etc.
Counsellors	• the safe storage and handling of student counselling records
Director of People and Culture	• managing staff requests for access to their personal information or employee records • the safe storage and handling of staff personal information or employee records • the safe storage and handling of personal information or employee records of prospective employees or unsuccessful candidates • the safe storage and handling of personal information or employee records of independent contractors
Finance Office	• the safe storage and handling of student financial details; student correspondence • the safe storage and handling of payroll records; financial records
Heads of School	• the safe storage and handling of student assignments and other assessed works • the safe storage and handling of course details
Management Committee	• takes responsibility for risk assessment in relation to record-keeping, taking decisions and implementing changes where needed to minimise risks and address hazards identified
Registrar	• supervising students who wish to access their personal records
Registrar's Office	• the safe storage and handling of student personal details, student academic details, student correspondence, academic results, student personal files, student administration archives
Staff	• maintaining accurate student records that relate to their School or Department • the safe storage and handling of student assignments and other assessed works; student correspondence

4 Definitions

For the purpose of this policy framework, the following definitions apply.

Term	Definition
cookie	A small text file which is placed on a computer's hard drive by some websites to store information about a visit to a website. A cookie only identifies the computer to a web server when there is a visit to the site; cookies do not identify users.
data breach	Occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. A data breach may be

	caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems. Examples of data breaches include: • loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information • a database with personal information is hacked • personal information is mistakenly given to the wrong person • unauthorised access to personal information by an employee • a breach that is likely to result in serious harm to any of the individuals to whom the information relates • a breach where the entity has been unable to prevent the likely risk of serious harm with remedial action • inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person • disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.
eligible data breach	The College is required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of eligible data breaches under the Notifiable Data Breaches scheme in Part IIIC of the *Privacy Act 1988* (Cth). An eligible data breach occurs when the following criteria are met: • There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur). • This is likely to result in serious harm to any of the individuals to whom the information relates. • The entity has been unable to prevent the likely risk of serious harm with remedial action. If it is not clear if a suspected data breach meets these criteria, the College must conduct an assessment to determine whether the breach is an 'eligible data breach' that triggers notification obligations.
employee records	Defined in the *Privacy Act 1988* (Cth) as a record of personal information relating to the employment of the employee.
important records	Records that can only be reproduced at considerable expense, time and labour. Important records include: • student and staff files • minutes of Management Committee • class records including enrolments, attendance records, results • teaching materials including unit outlines, lecture notes, study guides, readers • College publications, e.g. handbooks, course information books, etc.

	• current calendars and timetables.
learning management system (LMS)	A software application for the administration, documentation, tracking, reporting, automation, and delivery of educational courses, training programs, materials or learning and development programs. The College's LMS is known as ExO (Excelsia Online).
personal information	Defined in the *Privacy Act 1988* (Cth) as being information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is: a. true or not b. recorded in a material form or not. Information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result. Personal information includes, for example, names, addresses, telephone numbers, email addresses, dates of birth and passport numbers.
sensitive information	Information that is of a sensitive nature, including information about health, genetics, biometrics or disability; racial or ethnic origin; religious, political or philosophical beliefs; professional association or trade union memberships; sexuality; or criminal record. Special requirements apply to the collection and handling of sensitive information.
serious threat	As per the *Privacy Act 1988,* a serious threat is one that poses a significant danger to an individual or individuals. The likelihood of a threat occurring as well as the consequences if the threat materialises are both relevant. A threat that may have dire consequences but is highly unlikely to occur would not normally constitute a serious threat. On the other hand, a potentially harmful threat that is likely to occur, but at an uncertain time, may be a serious threat, such as a threatened outbreak of infectious disease. This allows the College to take preventative action to stop a serious threat from escalating before it materialises. This permitted general situation applies to a serious threat to the life, health or safety of any individual, or to public health or safety. The permitted general situation would not apply after the threat has passed. The permitted general situation applies to a threat to life, health or safety. This can include a threat to a person's physical or mental health and safety. It could include a potentially life-threatening situation or one that might reasonably result in other serious injury or illness. The permitted general situation would not ordinarily extend to a threat to an individual's finances or reputation. The threat may be to an individual the College is dealing with or to another person. It may also be a threat of serious harm to an unspecified individual, such as a threat to inflict harm randomly. A 'serious threat to public health or safety' relates to broader safety concerns affecting a number of people. Examples include: • the potential spread of a communicable disease

	• harm, or threatened harm, to a group of people due to a terrorist incident • harm caused by an environmental disaster. If time permits, attempts could be made to seek the consent from the relevant individuals for the collection, use or disclosure of personal information or data.
student management system	A software application that supports the key operational areas of education providers. It includes a comprehensive set of standard features to cover all aspects of student administration. The College uses Paradigm as its student management system.
vital records	Vital records include documents that: • prove ownership of property, equipment, vehicles and products • record how the College operates • document governance decisions, policies, goals and planning • document curriculum and course development • any other records whose absence would severely impede the function of the College. Examples of vital records include: • deeds and certificates of title • insurance policies • contracts and agreements • financial records • minutes of the Board of Directors and the Academic Board • proof of registration, certifications, approvals and accreditation of courses • curriculum and course development records • student data, including enrolment data, results, transcripts, etc. • alumni data and the Graduation Register.
web beacon	An image that originates from a third-party site to track visitor activities.

5 Procedures

The below procedures concern the storage and handling of information gathered by lawful means to facilitate the College's academic endeavours.

5.1 Storage and handling of student records

Category	Source	Storage	Access	Security	Retention
Personal details (name, address, contact numbers, gender, age, citizenship, educational background, work details, personal statement, references)	Course application forms and supporting documents	Digitised data is held on web-hosted student database with daily off-site backup	Student in Registrar's presence; staff as needed for duties	Digital files held in web-hosted student database with restricted password-protected access. Hard copies held in locked filing cabinets in the Registrar's Office. The Registrar's Office is locked and alarmed when staff are not in attendance	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College
Working with Children Check records	Course application forms, placement forms	Digitised data is held in Sharepoint or Asana with daily off-site backup	Placement Coordinators, Heads of School	Digital files held in SharePoint and Asana with restricted password-protected access	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College
Financial details (scholarship and/or financial assistance applications, invoices and payments associated with course delivery and student housing, payment contracts and student housing contracts)	Special application forms and supporting papers, documents indicating decisions, copies of financial transactions	Individual student file folders in filing cabinets in Administration, electronic records on database	Hard copies: student in Administrator's presence, staff as needed for duties. Electronic data: Key staff in student academic and financial administration	Hard copies held in locked filing cabinets in Registrar's Office. Access to student management system has levels of security, with change rights being restricted to key staff	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College

Academic details (enrolment, attendance and assessment details related to student's progress through the course, record of studies, transcript, testamur)	Forms created on database (some manually completed), printed testamurs	Individual student records held in file folders in filing cabinets in Administration, electronic records on database, class records filed in class folders on filing cabinets	Hard copies: student in the presence of Academic Registrar or Assistant Registrar, staff as needed for duties. Electronic data: Heads of Schools (read only), student administrators (change). Class files: Academic administrators, academic staff as needed for duties	Hard copies held in filing cabinets in Registrar's Office that are locked at day's end. Access to the student management system has levels of security, with change rights restricted to key staff in student academic and financial administration. Class files are sighted by staff as needed, in the Registrar's presence	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College
Assignments, exams and other assessed works	Student-generated work in hard copy and/or computer disks	Assessed work is usually held in temporary storage pending moderation and appeals. Distance education assessments are transmitted and returned electronically via the learning management system	Registrar's Office, Student administrators, , Heads of Schools, academic staff	Access is controlled by the Academic Registrar, Chief Academic Officer and Heads of Schools and is limited to academic staff or moderators as needed	12 months from the date on which the grade decision was made (unless relating to a complaint or appeal)
Correspondence; file notes; decisions in relation to applications for admission, credit, student housing, scholarships, financial assistance, appeals, amended grades	Letters, memos, file notes, electronic data on database	Mainly digitised and held electronically. Original signed class records held in class folders stored in bookcase and locked cupboard in Registrar's Office	Electronic data: student academic and financial administrators only. Class files: Staff of Registrar's Office and academic staff as needed for duties	Access to the student management system has levels of security, with change rights restricted to key staff. Class files are sighted by staff as needed, in the presence of student administrators	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College

Student grievances, complaints and misconduct record and evidence	Student Grievance application and supporting documentation, supplemented with other relevant student records	Mainly digitised and held electronically	Registrar's Office	Access is controlled by the Registrar's Office	7 years after last action
Learning Equity and Access Plan (LEAP)	Medical or health records	Digitised and held electronically	Disability Advisor	Access is controlled by the Disability Advisor	7–10 years from date of separation, whichever is later
Personal counselling records	Records related to student's candidacy and/or progress	Held in locked, coded files in the Counselling Centre	Counsellor only for students receiving counselling from a senior (employed) counsellor. If a student obtains counselling from a counselling intern (Master of Counselling student who counsels students from other schools under supervision), other key counselling staff may have access to the coded files.	Coded files are held in locked filing cabinets in the counsellors' offices. The Counselling Centre and counselling offices are locked when unattended	7–10 years from date of separation, whichever is later

5.2 Storage and handling of student archives

Category	Source	Storage	Access	Security	Retention
Academic results for each class	Hard copy files containing attendance records, results, unit outlines and student feedback. Student results also held electronically in student management system	Stored online in learning management system. Older documents stored in locked results cupboard in Registrar's Office	Registrar's Office staff as needed for duties	Archive room is kept locked, with keys held in the Finance and Facilities Office. Student management system access is by individualised security permissions	Folders are archived in locked storage for a minimum of 12 months. Online records held indefinitely

Student personal files	Student files containing complete personal information and academic history	Older files are kept in archive storage. Otherwise all personal files are kept online in student database	Registrar's Office staff as needed for duties	Archive room is kept locked, with keys held in the Finance and Facilities Office. Student management system access is by individualised security permissions	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College
Student administration archives	Handbooks; graduation files	Older files are kept in archive storage. Otherwise kept online in SharePoint	Registrar's Office staff as needed for duties	Archive room is kept locked, with keys held in the Finance and Facilities Office. SharePoint access is by individualised security permissions	Records are required to be retained for as long as the College continues to provide services to that student and for seven years after that student leaves the College

5.3 Storage and handling of staff records

Category	Source	Storage	Access	Security	Retention
Personnel files/employee records	All employment documents, including contracts, curriculum vitae, certified qualifications, position descriptions, reviews, WWCC, Police checks etc	Staff personal information is saved and backed up on SharePoint and PeopleStreme. Personnel folders and achieve folders are held in locked cabinets in the archive room and in offices	Management staff as needed for duties	Locked cabinets with COO and Director of People and Culture holding keys and supervising access. SharePoint access is by individualised security permissions. Files of former staff held in locked storage (archive room), locked office cabinets and SharePoint	Records must be kept for a minimum of 7 years

Payroll records	Staff contracts and online forms	Outsourced to Preceda cloud document storage	All staff access to personal information Payroll staff as needed	Password-protected access Access rights based on security settings	Records must be kept for a minimum of 7 years
Staff grievances, misconduct, complaints and worker's compensation	Staff Grievance application, complaints documents and incident reports and worker's compensation forms and supporting and relevant documentations	All documents stored in SharePoint folder, electronically	COO and Director of People and Culture	COO and Director of People and Culture access a secured file on SharePoint. Access to documents is controlled by COO	Records must be kept for a minimum of 7 years
Recruitment records	CVs, interview guides and assessment tasks	Saved and backed up on SharePoint and PeopleStreme	People and Culture staff and Recruitment Committee	SharePoint and PeopleStreme access is by individualised security permissions	Records must be kept for a minimum of 7 years

5.4 Storage and handling of course materials

Category	Source	Storage	Access	Security	Retention
Course details – structures and curricula	Course accreditation documents	Digitally on SharePoint	Head of School, CAO	Digital files held in SharePoint with restricted access and backed up off-site daily	Permanent – Do not destroy
Course details – course information books	Compiled publications	Electronically on Sharepoint, website. Also published as printed booklets. All formats controlled by issue and date	Digital copies available on website, SharePoint. Hard copies available onsite and on request	Original digital files held in SharePoint with restricted access and backed up off-site daily. Digital files published and updated on website	Permanent – Do not destroy

Course materials – study guides, readers, etc.	Heads of School, Academic staff, Academic Administrative staff, CAO	Held electronically on SharePoint and uploaded to the learning management system.	Available to enrolled students and teaching staff. Copyright restrictions on use.	Original digital files held and updated in School's SharePoint folder with restricted access. Published in digital format on the learning management system	Permanent – Do not destroy

5.5 Storage and handling of other vital documents

Category	Source	Storage	Access	Security	Retention
Contracts, deeds, insurance policies	Signed/authorised documents which may be received electronically or in print.	Electronically on SharePoint Hard copy originals held in cabinet onsite	Chief Executive, delegated management staff as needed	Digital files held in SharePoint with restricted access and backed up on the cloud. Hard copy originals held in cabinet onsite	Permanent – Do not destroy
Financial records	Digital records	Electronically on externally hosted database.	Finance staff	Records held in web-hosted database with daily off-site backup	Records must be kept a minimum of 7 years.
Proof of provider accreditation, registration, certification, etc.	External authorities, received in both hard and soft copy.	Electronically on SharePoint. Hard copy originals held in cabinet.	Chief Executive, delegated management staff as needed	Digital files held in SharePoint with restricted access and backed up on the cloud. Hard copies held in cabinet.	Permanent – Do not destroy
Proof of course accreditation, registration, certification, etc.	External authorities, received in both hard and soft copy.	Electronically on SharePoint. Hard copy originals held in cabinet.	Quality Office	Digital files held in SharePoint with restricted access and backed up on the cloud. Hard copies held in cabinet.	Permanent – Do not destroy

5.6 Responding to data breaches

Refer to the Data Breach Response Plan in PLA-GOV-02 Operations Continuity Plans.

5.7 Risk management

Once a year the Chief Financial Officer will:

1. review past disasters, looking at incidents that put records at risk and at the remedial measures that were taken.
2. survey areas where records are kept to identify further preventive actions that could be taken, e.g. in relation to light, dampness, fire hydrants, tidiness, etc.
3. review the appropriateness of staff access to each storage area.

The Chief Financial Officer will report on this survey to the Management Committee, and take steps to minimise hazards identified in storage areas.

The Management Committee will take responsibility for risk assessment in relation to record-keeping, taking decisions and implementing changes where needed to minimise risks and address hazards identified.

6 Document status and governance

Responsible Officer	Chief Executive Officer	Date created: October 2023 Date of last review: October 2023
Approving Authority	Management Committee	Meeting date: 13 October 2023 Agenda item number: 1.1
Publication	Version 1 (Public)	October 2023
Related documents and references	**External documents** Australian Privacy Principles *Child Protection (Working with Children) Act 2012* (NSW) *Criminal Code Act 1995* (Cth) FairWork Ombudsman Health Care Complaints Commission *Health Records and Information Privacy Act 2002* (NSW) *Higher Education Act 2001* (NSW) *Industrial Relations Act 1996* (NSW)	

	Information and Privacy Commission NSW *National Health Act 1953* (Cth) NSW Government Information Classification, Labelling and Handling Guidelines NSW Industrial Relations Office of the Australian Information Commissioner *Privacy Act 1988* (Cth) *Privacy and Personal Information Protection Act 1998* (NSW) *Telecommunications Act 1997* (Cth) *Workplace Surveillance Act 2005* (NSW) **Internal documents** Learning Equity & Access Plan Medical Practitioner Report Learning Equity and Access Plan Student Request for Access to Own Personal Information	
HESF	1.1, 1.2, 1.3, 1.4, 1.5, 2.2, 2.3, 2.4, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4, 6.1, 6.2, 6.3, 7.3	
Review date	Review of Version 1	October 2026

7 Document history

This policy framework has been amended as follows:

Version	Approved by and date	Sections amended