Privacy Management Plan

Section 1 - Purpose

(1) The Privacy Management Plan sets out commitments, obligations and responsibilities for managing and protecting the personal and health information held by Charles Sturt University (the University). The plan is developed to meet the requirements of the Privacy and Personal Information Protection Act 1998 and is intended to ensure that the University's obligations under the following legislation are understood and met:

a. Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
b. Privacy and Personal Information Protection Regulation 2019 (NSW)
c. Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)
d. Privacy Act 1988 (Cth)
e. Privacy (Tax File Number) Rule 2015 (Cth)
f. Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
g. Higher Education Support Act 2003 (Cth)
h. European Union General Data Protection Regulation 2016/679 (GDPR)

(2) This plan has the effect of a policy.

Scope

(3) This plan applies to all personal and health information of staff, students and members of the public held by Charles Sturt University (the University) and its controlled entities.

Section 2 - Policy

What the plan covers

(4) The Privacy Management Plan is divided into the following parts:

a. Part A sets out the privacy legislation and obligations that apply to the University and describes the personal and health information held by the University.
b. Part B outlines how the University complies with the information privacy principles, the health privacy principles and the Australian privacy principles set out in the PPIP Act, HRIP Act and Privacy Act 1988.
c. Part C outlines how the university complies with the GDPR In circumstances where the GDPR applies to the University's activities.
d. Part D explains how to contact the University regarding any privacy questions or concerns, and how these will be dealt with.
e. Part E sets out how this plan and privacy requirements will be communicated.

Part A - Overview of privacy obligations and information collected

Compliance obligations

(5) The University has compliance obligations in relation to privacy under the following legislation, regulations and other compliance drivers:

a. The Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) sets out the information protection principles (IPPs) that regulate how the University can deal with personal information of individuals, as well as other obligations. See Part B of this plan and the compliance register for more information about obligations under this Act.
b. The Health Records and Information Privacy Act 2002 (NSW) (HRIP Act) sets out the health privacy principles (HPPs) that regulate how the University can deal with health information. See Part B of this plan and the HRIP Act compliance overview for more information about obligations under this Act.
c. The Higher Education Support Act 2003 (Cth) (HESA) requires the University to comply with the Australian privacy principles (APPs) in Schedule 1 of the Privacy Act 1988 when handling students' personal information obtained for the purposes of chapters 3 and 4 of HESA (which are about assistance to students such as HECS-HELP and repayment of loans). See Part B of this plan and the compliance register for more information about obligations under this Act.
d. Some University professional staff are bound by professional codes of practice in relation to personal information they collect, including Australian Health Practitioner Regulation Authority (Ahpra), ministers of religion and archivists.
e. The Australian Research Council and the National Health and Medical Research Council require consideration of the privacy of research participants in:
    i. National Statement on Ethical Conduct in Human Research 2023, and
    ii. Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders 2018.
f. The Privacy Act 1988 requires that the University, as a file number recipient, comply with rules relating to tax file number information issued under section 17 of this Act, because it holds records of employees and students which contain tax file number information. See the compliance register for more information about obligations under this Act.
g. The General Data Protection Regulation (GDPR) in the European Union (EU) covers personal data collection and the privacy of EU residents. The GDPR will apply to the University if it meets specific criteria such as providing goods and services to EU residents or if it collects and/or processes personal data of EU residents. In circumstances where the GDPR applies to the University's activities, or where the University enters into a contract requiring it to comply with the provisions of the GDPR.
h. Advertising Council Australia's codes and regulations are complied with for the purpose of marketing and promotions.
i. A number of University policies set requirements for how personal information must be handled, including:
    i. Code of Conduct
    ii. Enrolment and Fees Policy (with regards to student's authorising third parties and representatives)
    iii. Records Management Policy
    iv. Information Technology Policy and Information Security Guidelines
    v. Student Misconduct Rule 2020
    vi. Information Technology Procedure - Personal Data Breach
j. In some instances, contracts and funding agreements may require the University to comply with the Privacy Act 1988 and the APPs as though it were an organisation within the meaning of this Act.

Personal and health information collected by the University

(6) The functions of the University are set out in section 7 of the Charles Sturt University Act 1989 (NSW) and include functions relating to the promotion, within the limits of the University's resources, of scholarship, research, free inquiry, the interaction of research and teaching, and academic excellence.

(7) To achieve these functions, the University collects the following types of personal information:

a. For past and present students and alumni:
    i. Personal identifiers (e.g. names, student ID numbers, contact details).
    ii. Digital photos for ID cards.
    iii. Financial information (e.g. tax file numbers, HECS-HELP loans).
    iv. Assessment information (e.g. academic results).
    v. Information collected under the Genuine Temporary Entrant requirements for international students (e.g. passport, sponsor details, family details).
b. For staff, including honorary, visiting and adjunct staff:
    i. Personal identifiers (e.g. names, staff ID numbers, contact details).
    ii. Digital photos for ID cards.
    iii. Financial information (e.g. tax file numbers, banking details, remuneration and superannuation details).
    iv. Previous employment details, staff communications.
c. For external persons:
    i. Personal identifiers (e.g. names, contact details) of individuals associated with the University such as benefactors, sponsors, consultants, contractors, suppliers and users of University facilities and services.
    ii. Financial information (e.g. banking details of contractors, suppliers).
    iii. Information provided by alumni and philanthropic donors (e.g. family relationships, philanthropic activities).
    iv. Some records of University governance bodies (particularly Council, Academic Senate and subcommittees) may refer to personal information relating to external persons.

(8) The main kinds of health information managed by the University include the following:

a. Medical records of patients receiving health services from University clinics, counselling services etc.
b. Student welfare information that is provided for the purpose of receiving counselling services or disability services, or with applications for special consideration, leave of absence or appeals (e.g. health and medical information, disability and equity information).
c. Staff welfare information (e.g. health and medical information related to employment including sick leave documentation, workers compensation and WHS files, and equity information).
d. Vaccination records or other health records as required by legislation in relevant jurisdictions.

What is not considered personal information

(9) The following categories of information are not considered personal information for the purpose of this plan:

a. Information that relates to a person who has been dead for more than 30 years.
b. Information that is publicly available.
c. Information about an individual that is contained in a public interest disclosure within the meaning of the Public Interest Disclosures Act 1994 (NSW), or that has been collected in the course of an investigation arising out of a public interest disclosure.

d. Information that relates to a person's suitability for employment as a public sector official.
e. Information that is de-identified, for which identifiers have been permanently removed or never included.
f. Information about University graduates, including a graduate's name, academic award, and year of conferral, which is made publicly available through the University's Alumni website.
g. Cookies and website tracking data, which can be used to identify the IP addresses and browsers of visitors to the University website, but do not identify individuals.

Part B - Application of privacy principles

(10) The following Part sets out how the University collects, stores and manages personal information in compliance with the privacy principles stated in:

a. Part 2 Division 1 of the Privacy and Personal Information Protection Act 1998 (referred to as information privacy principles, IPP 1-12).
b. Schedule 1 of the Health Records and Information Privacy Act 2002 (referred to as health privacy principles, HPP 1-15).
c. Schedule 1 of the Privacy Act 1988 (referred to as Australian privacy principles, APP 1-13).

Privacy risk assessments (PRAs) and privacy impact assessments (PIAs)

(11) Incorporating completion of a privacy risk assessment (PRA) and, if required, a privacy impact assessment (PIA) into the University's risk management framework demonstrates that the University has properly considered privacy, has robust and effective privacy practices, procedures and systems, and helps to create stakeholder trust.

(12) If a University project will involve the handling of personal information, a PRA will be completed. Examples of projects where a PRA should be considered are:

a. new technology that will collect and/or store personal information
b. integrating databases
c. engaging a third party to handle the Personal Information of the University.

(13) The greater the project's complexity and privacy scope, the more comprehensive the PRA and, if required, PIA should be to determine and manage the project's privacy impacts.

(14) PRAs and PIAs must also be completed for any activities to which the foreign privacy legislation, such as the GDPR, may apply. (Refer to Part C).

Collection of information

Collection for lawful purposes (IPP 1, HPP 1 and APP 3)

(15) The University will limit the collection of personal information to that which is reasonably necessary to enable the University to fulfil its lawful purposes. Health information will only be collected for a lawful purpose, directly related to the University's activities and necessary for that purpose.

(16) The following are examples of how personal information may be collected by the University and the advice that will be provided to individuals:

a. Forms and websites used by the University to collect personal information will include a statement that explains the purpose for which the personal information is being collected.
b. Students, staff or other clients seeking counselling or similar services within the University will be advised that

personal information will be collected as part of the service they are seeking.

c. Personal information collected during a verbal conversation and recorded by a University staff member or representative is collected, stored and disclosed in line with this plan.
d. Students who are to be recorded (as video or audio) in the course of their studies, including during online examinations invigilated by University staff on mediums such as Zoom (outside of general lecture recordings) will be told how the recordings will be used, stored, disclosed (or not) and disposed of and how they can gain access to the recording.
e. People are invited to leave messages on telephone answering machines or to send email messages and they could be identified from such messages. The telephony system allows for voicemail messages to be forwarded by email to a third party. These practices are not contrary to IPP 1.
f. Some groups record (as video or audio) classes, workshops and professional development activities and use the tapes to provide feedback to participants. All such recording is done with the knowledge and permission of the participants involved and is not in breach of the IPPs. Participants will be advised as to how the information will be collected, used, stored, disclosed to others and disposed of.
g. Automated electronic systems log the use by staff, students and other users of the University's computer networks and systems, for the purpose of monitoring and ensuring compliance with the Information Technology Procedure - Acceptable Use and Access. The University uses this information from time to time as evidence in cases of alleged breaches of the policy. Users are required to acknowledge their awareness that a record is kept of their usage of the facilities for the sole purpose of monitoring their compliance with the policy as evidenced by an acknowledgment required each time their password is changed.
h. The University's communications management system logs transactions between the University and prospective students, current students and alumni. This data may be used to map a person's activities for the purpose of providing services to prospective students, students and graduates. These practices are not contrary to IPP 1.

Collection from the person concerned (IPP 2, HPP 3)

(17) As required by IPP 2, most personal information collected by the University is collected directly from the person to whom it relates, except where the person authorises the collection of information from another source, or a parent or guardian provides information for a person under 16 years of age.

(18) The following are examples of where personal information may be collected from other sources and are not considered contrary to IPP 2:

a. A prospective student's academic record may be obtained from other bodies, as consented to by the student signing a statement on the admission application form.
b. Referee checks for people seeking appointment as staff of the University or from staff seeking promotion. The person's permission is obtained to do this.
c. Staff, and students in specific courses, may be required to undergo criminal history checks from the Australian Federal Police (National Police Check), NSW Police Force, or other relevant jurisdictions.
d. Staff and students (subject to their course requirements) who are required to work with children or vulnerable people may be also required to undergo criminal history checks. These clearances are authorised under the Child Protection (Working with Children) Act 2012 (NSW), or applicable legislation in relevant jurisdictions.
e. Background screening will be completed, in accordance with Australian standard AS 4811-2006, to confirm the identity, integrity and credentials of people with certain positions and duties. These may apply to current or prospective staff, contractors and consultants, and will only be completed with the person's consent.
f. The University sometimes collects personal information such as name and email address from school students, who may be under 16 years of age, in order to provide them information about the University and its courses. This personal information is used for no other purpose other than that for which it is collected or for quality

assurance purposes.

g. The University may obtain current contact details of the University's graduates from third parties or social media sites in order to offer those graduates the opportunity to maintain contact with the University and access alumni services.
h. The University may obtain current contact details of students of the University from third parties or applicants to the University without their knowledge or permission. The information is used to maintain contact with those persons to offer services of the University.
i. The University may, in investigating alleged misconduct or breaches of University rules and policies, obtain personal information about students or other persons from third parties without the permission of the parties to the matter. To the extent necessary, the person is provided with an opportunity to respond to the information provided as required by the rules and processes relating to alleged misconduct.
j. Some organisational units receive reports on students undertaking professional practice placements in schools, hospitals and other government and non-government organisations. Students are usually advised in their handbook or subject outline, or would reasonably be expected to know, that personal information regarding their performance would be collected.

Requirements for collection - open (IPP 3, HPP 4)

(19) As far as practicable, the University will inform students, staff and other individuals why the information is being collected and how it will be used, at the point of collection:

a. The University's forms and websites used to collect personal information will include a statement directing respondents to this plan.
b. Most organisational units do not specifically advise people that they are being asked to provide information of their own free will, but people could reasonably be expected to know that they were providing their personal information freely.
c. The University contracts with organisations outside of the University and uses service providers with locations in various countries to process, use or store the personal information of its students and staff. The University will transfer personal information of its students and staff in a way that is consistent with applicable legal requirements and only to the extent that is necessary for the purpose that it was collected and as outlined in this plan. The University may do this by asking for evidence of information handling processes from such service providers and by inserting an appropriate privacy clause into the relevant contract to ensure the University complies with its obligations under the PPIP Act.

(20) In some instances, personal information may be disclosed to third parties, either under statutory requirements and/or with the person's knowledge and permission:

a. Personal information relating to students is provided to Commonwealth agencies, including:
    i. Department of Education, Skills and Employment
    ii. Department of Home Affairs
    iii. Australian Tax Office
    iv. Department of Human Services
b. Personal information relating to staff may be made available to outside organisations, usually with the permission of the staff member or as required by law. For example, salary details are provided to the staff member's bank for the payment of salary and certain personal information is supplied to corporate credit providers for staff who are issued corporate credit cards.

Requirements for collection – relevant and accurate (IPP 4, HPP 2)

(21) Most personal information and health information is provided by the person to whom it relates and is therefore

assumed to be accurate, relevant, not excessive and not an unreasonable intrusion. University policies (e.g. Enrolment and Fees Policy) stipulate that students are responsible for the accuracy of their personal information and are able and encouraged to amend their personal information as it changes.

(22) In some instances, personal information of staff or students is required to be verified before decisions are made. This verification would include contacting referees before appointing or promoting staff and verifying the academic and other qualifications of students seeking enrolment at the University. In cases of alleged misconduct involving staff or students, there are prescribed processes for establishing the provenance of relevant personal information.

(23) Organisational units only collect personal information that is directly related to the work of the unit.

(24) The University seeks to minimise unreasonable intrusion to an individual and not collect and store excessive personal information or health information. For this reason:

a. personal information that is shared between systems and organisational units will be limited to only the information that is necessary for the functions and operations of the system or service,
b. health information will not be shared between systems and organisational units, and
c. individuals may be asked on multiple occasions to provide personal and/or health information to different organisational units and systems. This practice is considered necessary to ensure that their personal or health information records held by the University are up to date and accurate.

Storage of information

Retention and security (IPP 5 and HPP 5)

(25) The University will hold personal and health information securely and retain it for the periods required under the State Records Act 1998 (NSW). Personal information will be kept for no longer than is necessary for the purposes for which the information was collected and will be disposed of securely and in accordance with any requirements for the retention and disposal of personal information.

(26) Most of the University's organisational units store personal information on computers or on file servers. Access to this information is protected by passwords that are issued and controlled by the Division of Information Technology.

(27) Personal information held on the University's primary information systems for student, finance, personnel and corporate records is protected against unauthorised access, modification or disclosure by additional security levels that control access and functionality accorded to the various users of the systems.

(28) The Division of Information Technology is responsible for ensuring that the University's electronic records are regularly backed up and otherwise protected against loss or damage.

(29) Where third party operating systems are used to hold personal information, contracts must include provisions for security, retention and disposal of the information in accordance with the University's legislative responsibilities. Specifically, the University will ensure that third party contracts incorporate appropriate obligations to ensure compliance with PPIP Act (and to the extent applicable, any other privacy laws) and this Privacy Management Plan. In these cases, the area of the University responsible for managing these activities or contract must complete a privacy impact assessment (PIA) beforehand to ensure the activity meets privacy obligations.

(30) The disposal of personal information is managed in accordance with the State Records Act and the approved general retention and disposal authorities (GDAs):

a. GDAs relevant to the University are listed on the Records Management website.
b. Disposal of information must be documented and approved in accordance with the Records Management Policy.

Access and accuracy

Information about the information held (IPP 6 and HPP 6)

(31) In addition to the general information provided in this plan, individuals may contact the Privacy Officer for information about what personal and health information is being stored about them, how it is being used and any rights regarding access to the information, via the University's Privacy and your information webpage.

Access to information (IPP 7 and HPP 7)

(32) The Records Management Policy (and associated procedures) set out how students and staff can access their personal information, generally at no cost (subject to some limitations). See also Part D below which outlines how an individual can access information held about them in some circumstances.

Alteration of information (IPP 8 and HPP 8)

(33) The University encourages students or staff to keep their personal information and contact details up-to-date, this includes the right to annotate and correct information held by the University. Part D sets out how an individual can access and correct information held about them.

Use of information

Checking information before use (IPP 9 and HPP 9)

(34) Much of the personal information collected by organisational units either does not change or changes only occasionally (for example, name, date of birth, marital status, gender, ethnicity). The University does not routinely check this type of information before using the information.

(35) Some personal information is checked as a matter of course soon after its collection. For example, students' enrolment each session is confirmed with them as their enrolment load determines the amount of HECS-HELP or fees for which they are liable. Students must also confirm their personal information held when enrolling in subjects each teaching session in order to progress the enrolment process.

Limits on use of information (IPP 10 and HPP 10)

(36) Personal and health information collected by the University will only be used for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to a person's health or safety.

(37) The use of personal information for statistics and quality assurance purposes is considered to be related to the purpose for which the information was collected (for example, to improve the quality of services provided by the University). The Office of Planning and Analytics may receive personal information that it will provide to other organisational units in an aggregated or de-identified format. Where an organisational unit requests identified information, executive approval must confirm that the information is required to meet a genuine business need.

Limits on disclosure of information (IPP 11, HPP 11 and HPP 14)

(38) The disclosure of personal and health information will be limited by the University and restricted to the purpose for which it was collected unless an exemption applies under a relevant privacy legislation or code of practice.

(39) As part of its routine management tasks, some organisational units disclose personal information to bodies outside NSW, usually at the request of the person concerned. This includes:

a. for staff or students seeking positions in interstate or overseas organisations,
b. for students undertaking fieldwork placements interstate, and/or

c. sending personal information relating to staff and international students to affiliated institutions of the University that deliver the University's courses in locations outside of NSW and Australia.

(40) When requested, Student Administration will verify whether a named person has received a qualification from the University, or aspects of their academic performance, to an individual or body demonstrating justifiable reason, for example, at the request of a prospective employer of a graduate to check a claim for employment. The award of qualifications is a public act. Verifying to a third party whether a person has obtained a particular qualification from the University, their academic performance during their studies (e.g. their grades in a subject) and the publication of their name and conferred qualification does not contravene the IPPs.

Sensitive information (IPP 12)

(41) There are stricter obligations for the disclosure of personal sensitive information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health and sexual activities. The University will only collect personal sensitive information on a voluntary basis, or where it is required to do so by law. The University will only disclose this information with the consent of the person, or when required to do so by law, or if the disclosure is necessary to prevent or minimise a serious or imminent threat to the person’s health or safety.

(42) Examples of where this information may be collected and/or disclosed with the individual’s permission include but are not limited to:

a. to access targeted University programs, services and support (e.g. First Nations staff and student programs, disability support services),
b. applications for special consideration or sick leave,
c. as part of counselling sessions,
d. to organise reasonable adjustments for workplace learning for students with disabilities, or
e. to facilitate workplace learning allocations as required by host locations.

Identifiers and anonymity

Use of identifiers (equivalent to HPP 12, APP 9)

(43) The University issues a unique University number to all students and staff in order to carry out its functions.

(44) The University will not adopt, use or disclose a government related identifier unless authorised by or under an Australian law or a court or tribunal.

Anonymity and pseudonymity (equivalent to HPP 13, APP 2)

(45) Students and staff are not provided with the option of being known under a pseudonym or to be anonymous because:

a. the status of the testamur as an official document precludes the opportunity for a student to elect to not identify themselves or to be known under a pseudonym, and
b. as employees of a corporation established under statute, staff are not permitted to be anonymous or be known by a pseudonym.

Health linkage system (HPP 15)

(46) A health records linkage system is a computerised system designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records. The University does not currently use any health records linkage (such as My Health Record).

Exemptions

Serious and imminent threat

(47) The University may use personal information and disclose it to prevent or lessen a serious and imminent threat to a person's health or safety.

(48) This exception has been determined by the NSW Civil and Administrative Tribunal (NCAT) to be permitted in very limited circumstances. The threat must be both serious and imminent: imminent meaning likely to occur at any moment, or impending. There must also be a belief held on reasonable grounds about the serious and imminent threat by the officer of the University when this exception is relied on.

(49) Staff involved in assessing any threat should speak to their supervisor and also contact the University's Privacy Officer and/or the General Counsel for advice.

PPIP Act exemptions

(50) Division 3 of PPIP Act sets out the exceptions to compliance with IPPs. The exemptions relevant to University operations are set out below.

(51) These should not be read as an exhaustive list of exemptions and any University officer unsure whether an exemption applies when handling personal information in their role should discuss the matter with their supervisor or contact the University's Privacy Officer.

Investigations

(52) The University is not required to comply with the privacy obligations under section 24 of the PPIP Act if:

a. it is investigating or otherwise handling a complaint and compliance might detrimentally affect the proper handling of its investigative function, or
b. non-compliance is reasonably necessary to enable the University to exercise its complaint handling functions, or
c. the information is disclosed to an investigative agency.

Law enforcement purposes or otherwise lawfully authorised

(53) The University is not required to comply with the obligations under section 23 of the PPIP Act if:

a. the information is collected for law enforcement purposes, or
b. the information is collected in connection with any proceedings (whether or not actually commenced) before any court or tribunal, or
c. use of the information is reasonably necessary for law enforcement purposes or the protection of public revenue, or
d. disclosure of the information is:
    i. made in connection with proceedings for an offence or for law enforcement purposes, or
    ii. to a law enforcement agency for the purposes or ascertaining the whereabouts of a missing person, or
    iii. authorised or required by subpoena or by search warrant or other statutory instrument, or
    iv. reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe an offence may have been committed, or
e. disclosure of the information is reasonably necessary to assist in a state of emergency, or
f. the University is otherwise lawfully authorised or required not to comply with the PPIP Act, or non-compliance is permitted under any Act or law.

(54) A reference to ‘law enforcement purposes’ includes law enforcement purposes of any state or territory, or the Commonwealth, of Australia.

(55) Examples of other legislation which may authorise non-compliance include the GIPAA, the State Records Act 1998 (NSW) and the Data Sharing (Government Sector) Act 2015 (NSW). The operation of this and any other legislation that permits non-compliance with the PPIP Act does not affect the University's handling of the personal information and health information, other than for the purpose of the exempt conduct.

Public sector agencies

(56) There is often confusion between the operation of the Privacy Act 1988 (Cth) (the federal Privacy Act) and the PPIP Act and the HRIP Act. The University is defined as a ‘public sector agency’ under the PPIP Act and the HRIP Act and must comply with the privacy obligations arising under those laws, which are the University's primary privacy obligations.

(57) Under section 27A of the PPIP Act, a public sector agency is not required to comply with the information protection principles with respect to the collection, use or disclosure of personal information if:

a. the agency is providing the information to another public sector agency or the agency is being provided with the information by another public sector agency, and
b. the collection, use or disclosure of the information is reasonably necessary
    i. to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or member of Parliament, or
    ii. to enable inquiries to be referred between the agencies concerned, or
    iii. to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of agencies).

Research

(58) Under section 27B of the PPIP Act, there is an exemption that applies to the collection, use or disclosure of personal information used for research purposes, or the compilation or analysis of statistics in the public interest, provided that specific conditions are met. Staff engaged in research that wish to access personal information held by the University for research purposes should refer to the NSW Information and Privacy Commissioner's Statutory Guidelines on Research – For more information consult with the University's Privacy Officer or the General Counsel. Approval from the University's authorised delegate is required before any information can be provided.

(59) The University's Research Data Management Procedure specifies the responsibilities of the University, its researchers and research students regarding the management of research data.

Sensitive personal information

(60) The PPIP Act provides a restriction on disclosure for ‘sensitive’ types of information, which are defined as an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual activities. The University will not disclose this type of information unless it is necessary to prevent a serious and imminent threat to the life or health of an individual.

(61) It should be remembered that sensitive personal information may be contained in identification documents, such as passports and drivers’ licences. For example, photos might establish racial origin or religion and a document evidencing an individual’s marital status may disclose their sexual orientation.

Other exemptions

(62) The University is also exempt from various provisions of the PPIP Act where:

a. the individual concerned has expressly consented to non-compliance with particular provisions.
b. it discloses to or receives from another agency information about an individual in any of the circumstances described in section 27A of the PPIP Act, including for the purpose of enabling inquiries to be referred between the University and that other agency.
c. the collection, use or disclosure of the information is reasonably necessary for research and the matters in section 27B of the PPIP Act apply.

(63) The University may also have mandatory reporting obligations to regulatory bodies, such as the NSW Independent Commission Against Corruption (ICAC), and other government agencies.

Public registers

(64) The University publishes:

a. a register for verifying awards and qualifications conferred by the University, as described at clause 40. Individuals cannot opt out of this,
b. graduation material which includes the name of each graduate and the degree conferred upon them and may be made available to attendees at graduation ceremonies and online. Individuals may opt out of inclusion by contacting the University's Privacy Officer,
c. a Contract register as required by the Government Information (Public Access) Act 2009 (NSW) (GIPA Act). It is unlikely the register will include personal or health information,
d. a Disclosure Log as required by the GIPA Act. The disclosure log will not include personal or health information.

(65) Enquiries about the inclusion of personal information in a public register can be made to the University's Privacy Officer.

Part C - General Data Protection Regulations (GDPR) – additional provisions for privacy regulation of foreign countries

(66) Foreign privacy regulation, such as the GDPR, may apply to a variety of University activities including:

a. processing of personal information of staff, students and alumni located in the countries or area covered by the regulation, in respect of the GDPR it covers countries within the European Economic Area (EEA) and the United Kingdom (UK). (In the GDPR, 'processing' has a similar meaning to 'handling' and 'personal data' has a similar meaning to 'personal information')
b. where the University offers goods or services in countries or areas covered by the legislation, such as the EEA or UK, irrespective of whether payment is required (for example, where the University actively promotes programs to residents in those countries or areas)
c. where the University enters into a contract with an entity located in that country or area, which involves the processing of personal information and disclosure of it out of that country or area to the University, and vice versa
d. where the behaviour of individuals located in that country or area is being monitored or tracked, for example, using cookies on the website, and
e. in research collaborations with entities in that country or are which include collecting and processing personal data.

(67) Under some foreign privacy regulations, such as the GDPR, it is a requirement where information is collected, stored or disclosed as a result of express consent given by an individual, that consent may be withdrawn by that individual at any time.

(68) The individual may have the right to request the erasure, portability or restriction of processing of their personal data, and to object to the processing of their personal data.

(69) To request access, correction or erasure of personal information under the GDPR, please contact the University's Privacy Officer at: informationintegrity@csu.edu.au.

Part D - Inquiries, reviews and breaches of privacy

(70) Individuals have a right under the privacy statutes to request access to, and correction of, personal information held by the University.

(71) Staff, students and members of the public are encouraged in the first instance to contact the head of the organisational unit responsible for holding the personal information in question if they wish to:

a. know what personal information about them is held by the University,
b. know how their personal information is stored, used, disclosed or disposed of,
c. have their personal information corrected, or
d. express concern about any of the above matters.

(72) Individuals have the right to correct personal information held by the University if it is inaccurate, out of date, incomplete, irrelevant or misleading. The handling of a request to access or correct personal information will be at no cost to the individual seeking access to their personal information or to address a concern about their personal information.

(73) If the University is unable to provide access to or correct their personal information, the individual will be notified in writing of:

a. the reasons for refusing access or to correct the personal information,
b. their right to request that a statement be associated with their personal information (see clause 74), and
c. how they can lodge a complaint if they wish to.

(74) Where a request to correct personal information held by the University is refused, the individual may request that the University associate a statement with that information that the individual believes the personal information held is inaccurate, out of date, incomplete, irrelevant or misleading. The University must take reasonable steps to associate the statement with the individual's personal information so that the statement is apparent to users of the personal information.

(75) Organisational units may seek advice from the University Ombudsman, as the University's privacy officer, for advice on allowing access and corrections to the personal information they hold.

Internal review by the University

(76) A person who is aggrieved by the conduct of the University in relation to their personal information is entitled to a review of that conduct. An individual may

a. contact the organisational unit involved and/or the University's Privacy Officer and resolve the matter informally,
b. lodge an application applying for an internal review with the University's Privacy Officer into the use, storage or disclosure of personal information held about them as provided by Part 5 of the PPIP Act. The process and requirements as identified in section 53 of the PPIP Act will apply to internal reviews,
c. apply for an external review by the NSW Civil and Administration Tribunal (NCAT) or make a complaint to the

NSW Information Privacy Commissioner.

(77) An application for internal review must:

a. be in writing,
b. be addressed to the University's Privacy Officer,
c. specify an address in Australia to which a notice of the outcome may be sent,
d. be lodged with the University within six months from the time the applicant first became aware of the conduct (or a later date at the discretion of the University), and
e. comply with any other requirements prescribed by the law from time to time.

(78) The University's Privacy Officer will then either deal with the application directly and undertake the review, or will appoint another suitable person. Except as provided for in the PPIP Act, the person who deals with the application must, as far as practicable, be a person:

a. who was not substantially involved in any matter relating to the conduct the subject of the application, and
b. who is an employee or officer of the University, and
c. who is otherwise suitably qualified to deal with the matters raised by the application.

(79) The appointed person will review the conduct the subject of the application and complete the review in accordance with Part 5 of the PPIP Act. In reviewing the conduct of the subject of the application, the person appointed to deal with the application must consider any relevant material submitted by the applicant and the Privacy Commissioner.

(80) The internal review should be completed as soon as is reasonably practicable in the circumstances, and will usually be completed within 30 days.

(81) Following completion of the review, the University may do any one or more of the following:

a. Take no further action on the matter.
b. Make a formal apology to the applicant.
c. Take such remedial action as it thinks appropriate.
d. Provide undertakings that the conduct will not occur again.
e. Implement administrative measures to ensure that the conduct will not occur again.

(82) The University will notify the NSW Privacy Commissioner as soon as practicable after receiving an application for internal review, and keep the NSW Information Privacy Commissioner informed of the progress and findings of the internal review and the action proposed to be taken by the University in relation to the matter.

External reviews and complaints

(83) If an applicant for internal review is not satisfied with the findings of the internal review or the action taken by the University in relation to the application, they may make an application within 28 days to the NSW Civil and Administrative Tribunal (NCAT) for a review of the decision that is the subject of the application.

(84) Staff and students may also make a complaint to the NSW Information and Privacy Commission.

Breaches of privacy and unauthorised access to personal information

(85) A data breach occurs when personal information or data held by the University is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Suspected or confirmed data

breaches will be managed as set out in the Information Technology Procedure - Personal Data Breach.

(86) An eligible data breach occurs where:

a. there is an unauthorised access to, or unauthorised disclosure of, personal information held by the University, or there is a loss of personal information held by the University in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of the information, and
b. a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

Notifiable Data Breaches scheme (Cth)

(87) The Australian Government has established the Notifiable Data Breaches (NDB) scheme under the Privacy Act (Cth) to ensure that individuals are notified about serious breaches of their personal or health information. This scheme came into effect on 22 February 2018.

(88) The Notifiable Data Breaches scheme applies directly to the University in limited circumstances, and the University is only required to notify the Office of the Australian Information Commissioner (OAIC) where there is a data breach that involves tax file numbers.

(89) The Notifiable Data Breaches scheme applies to contractors and other organisations that the University does business with because they are subject to the Privacy Act (Cth). Some of these contractors and other organisations may have access to or store personal or health information on behalf of the University.

(90) The University is required to comply with the mandatory Notifiable Data Breaches scheme which includes notifying the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm to an individual to whom the personal or health information relates.

(91) The University is required to maintain an internal data breach incident register to comply with the mandatory Notifiable Data Breaches scheme.

Mandatory Notification of Data Breach scheme (NSW)

(92) The NSW Government established a Mandatory Notification of a Data Breach (MNDB) scheme under the Privacy and Personal Information Protection Act (NSW) that requires the University to provide notifications to affected individuals in the event of an eligible data breach of their personal or health information held by the University. This scheme came into effect on 28 November 2023.

(93) The University is required to comply with the MNDB scheme which includes notifying the NSW Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm to an individual to whom the personal or health information relates.

(94) The Privacy Officer must establish and maintain:

a. an internal data breach incident register, and
b. a public notification register for the recording of eligible data breaches. The information recorded in the register must be publicly available for at least 12 months after the date of publication.

(95) The Information Technology Procedure – Personal Data Breach outlines the procedures and practices used by the University to ensure compliance with the obligations and responsibilities set out in part 6A of the PPIP Act for the MNDB scheme.

University processes

(96) The University will establish processes for responding to data breaches and reporting notifiable data breaches in line with the requirements of the Privacy Act 1988 (Cth), PPIP Act and HRIPA and, where applicable, foreign privacy laws such as the GDPR.

(97) The University will incorporate standard provisions for all contracts with contractors and other organisations who handle personal or health information on behalf of the University. These provisions will include, as a minimum, requirements to:

a. implement systems and controls that comply with the relevant privacy laws, including any mandatory reporting schemes for data breaches,
b. allow the University to review or audit those systems and controls, and
c. notify the University and provide full details of any data breaches (including notifiable data breaches) in respect of any personal information held by that contractor or service provider as this relates to personal or health information held on behalf of the University.

Offences

(98) Individuals who intentionally breach, disclose or use any personal or health information about another person otherwise than in connection with the lawful exercise of their official functions commit an offence under part 8 of the PPIP Act and/or the HRIP Act. This may include:

a. disclosing or using personal or health information,
b. information that the individual has accessed, or
c. offering to supply or holding themselves out as being able to supply personal or health information that the person knows, or to reasonably know, has been or is proposed to in contravention of the PPIP Act and/or the HRIP Act.

Penalties include fines, imprisonment or both.

(99) The supervisory authority for the GDPR imposes fines and penalties that are effective, proportionate, and dissuasive. This may include but is not limited to:

a. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them,
b. the intentional or negligent character of the infringement,
c. any action taken by the controller or processor to mitigate the damage suffered by data subjects.

Part E - Training and awareness

(100) The obligations of the University and its staff as identified under the PPIP Act and HRIP Act will be the subject of information and training sessions conducted by the University's Privacy Officer and online training modules completed by staff. These information and training sessions and training modules will be designed to enhance staff awareness of privacy and cyber principles and current threat trends, in addition to training and awareness around identifying, responding to, and managing data breaches.

(101) General alerts will also be made on the University's communication systems to remind staff and students of their privacy protection obligations.

(102) The University’s privacy web page provides detailed information on how the University meets its obligations

under the privacy legislations, the Privacy and Personal Information Protection Act 1998 (NSW)and the Privacy Act 1988 (Cth) and the Health Records and Information Privacy Act 2002 (NSW).

(103) Where privacy-related matters are addressed in policies and procedures, the University's Privacy Officer is a core stakeholder in accordance with the Policy Development and Review Procedure and will be consulted when minor or major changes are proposed, to ensure compliance with the PPIP Act and HRIP Act and any other relevant legislation.

Contact information

(104) People seeking further information or advice regarding the matters contained in this plan can review the University's Privacy web page or contact the University's Privacy Officer.

Section 3 - Procedures

(105) Nil.

Section 4 - Guidelines

(106) Nil.

Section 5 - Glossary

(107) For the purpose of this plan, the following additional terms have the definitions stated:

a. Health information – means information or an opinion about the physical or mental health or a disability (at any time) of an individual, a health service provided or to be provided to an individual, or an individual's express wishes about health services provided to them in the future, or other personal information collected to provide, or in providing a health service, or as otherwise defined at section 6 of the HRIP Act.
b. Personal information – as defined in the PPIP Act, means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion, including things such as an individual's fingerprints, retina prints, body samples or genetic characteristics, but does not include certain information excluded under the PPIP Act.
c. Privacy impact assessment (PIA) - is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimizing or eliminating that impact.

Status and Details

Status	Current
Effective Date	20th June 2024
Review Date	13th January 2028
Approval Authority	University Secretary
Approval Date	20th June 2024
Expiry Date	Not Applicable
Unit Head	Anthony Heywood University Secretary
Author	Melanie Rumball University Ombudsman mrumball@csu.edu.au
Enquiries Contact	Melanie Rumball University Ombudsman mrumball@csu.edu.au