

# 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 \(NSW\) \(PIIP Act\)](#)
- 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 \(Cth\)](#)

(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 - Glossary

(4) 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 [PIIP 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 [PIIP Act](#).

## Section 3 - Policy

### What the plan covers

(5) 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 explains how to contact the University regarding any privacy questions or concerns, and how these will be dealt with.
- d. Part D sets out how this plan and privacy requirements will be communicated.

## Part A - Overview of privacy obligations and information collected

### Compliance obligations

(6) 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 [psychologists and counsellors](#), [health practitioners](#), 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 2007 \(updated 2018\)](#), 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. [Advertising Council Australia's codes and regulations](#) are complied with for the purpose of marketing and promotions.
- h. 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](#)

- i. 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**

(7) 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.

(8) 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.

(9) 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**

(10) 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

(11) 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).

### Collection of information

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

(12) 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.

(13) 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)**

(14) 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.

(15) 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)**

(16) 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 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](#).

(17) 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)**

(18) 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.

(19) 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.

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

(21) 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)**

(22) 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.

(23) 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.

(24) 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.

(25) 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.

(26) 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.

(27) 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)**

(28) In addition to the general information provided in this plan, individuals may contact the University Ombudsman 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 Ombudsman's webpage](#).

### **Access to information (IPP 7 and HPP 7)**

(29) 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 C below which outlines how an individual can access information held about them in some circumstances.

### **Alteration of information (IPP 8 and HPP 8)**

(30) 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 C 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)**

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

(32) 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)**

(33) 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.

(34) 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 (e.g. 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)**

(35) 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.

(36) 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.

(37) 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)**

(38) 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.

(39) 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)**

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

(41) 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)**

(42) 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)**

(43) 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**

(44) Exemptions in the [PPIP Act](#) and the [HRIP Act](#) that may be relevant to the University include:

- a. exemptions relating to law enforcement (section 23 of the [PPIP Act](#))
- b. exemptions relating to exercise of investigative functions (section 24 of the [PPIP Act](#))
- c. exemptions relating to information exchanges between public sector agencies (section 27A of the [PPIP Act](#))
- d. exemptions relating to research (section 27B of the [PPIP Act](#)).

## **Part C - Inquiries, reviews and breaches of privacy**

### **Request to access and/or correct personal information held by the University**

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

(46) 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.

(47) 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.

(48) 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 49), and
- c. how they can lodge a complaint if they wish to.

(49) 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.

(50) 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**

(51) 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 lodge an application for an internal review with the University's privacy officer – currently, the University Ombudsman – 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.

(52) 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, and
- d. be lodged with the University within 6 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.

(53) 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.

(54) 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.

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

(56) 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.

(57) The University will notify the NSW Privacy Commissioner as soon as practicable after receiving an application for internal review, and keep the NSW 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**

(58) 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. Details for contacting NCAT can be found on [their website](#).

(59) Staff and students may also make a complaint to the NSW Information and Privacy Commission. Details for contacting the NSW Information Privacy Commission can be found on [their website](#).

## **Unauthorised access to personal information**

(60) A data breach occurs when a failure causes or has the potential to cause unauthorised access to data, including personal information, held by the University. Suspected or identified breaches of personal information will be managed as set out in the [Information Technology Procedure - Personal Data Breach](#).

(61) The University is required to notify the Office of the Australian Information Commissioner (OAIC) where there is a data breach that may result in serious harm to the individual(s) affected or that involves tax file numbers.

## **Part D - Training and awareness**

(62) The obligations of the University as identified under the [PPIP Act](#) and [HRIP Act](#) will be the subject of information and training sessions conducted regularly by the University Ombudsman as the University's privacy officer. General alerts will also be made on University communication systems to remind staff and students of their privacy protection obligations.

(63) The University's [Privacy website](#) provides more detailed information on privacy for those who need more, and/or ongoing, information about privacy issues.

## **Contact information**

(64) People seeking further information or advice regarding the matters contained in this plan should contact the [University Ombudsman](#). Contact details are provided on the University's [Privacy website](#).

## **Section 4 - Procedures**

(65) Nil.

## **Section 5 - Guidelines**

(66) Nil.

## Status and Details

<b>Status</b>	Current
<b>Effective Date</b>	2nd December 2021
<b>Review Date</b>	2nd December 2024
<b>Approval Authority</b>	University Secretary
<b>Approval Date</b>	1st December 2021
<b>Expiry Date</b>	Not Applicable
<b>Unit Head</b>	Anthony Heywood University Secretary
<b>Author</b>	Melanie Rumball University Ombudsman mrumball@csu.edu.au
<b>Enquiries Contact</b>	Melanie Rumball University Ombudsman mrumball@csu.edu.au