Privacy Management Plan

Section 1 - Introduction

(1) This is the Privacy Management Plan (the Plan) of Charles Sturt University (the University) prepared as required by Part 3 Division 2 of the Privacy and Personal Information Protection Act 1998 (the PPIPA).

Section 2 - Objective

(2) The objective of the Plan is to facilitate the University's compliance with the PPIPA.

Section 3 - Methodology

(3) The Plan is a revision and update of the Charles Sturt University Privacy Management Plan as endorsed by the University Council on 17 August 2000 (CNL 00/166).

(4) This revised and updated Plan was developed by the University Ombudsman, considered by the Vice-Chancellor's Leadership Team, approved by the University Council, (the University's governing body) and submitted to the Privacy Commissioner.

Section 4 - Functions of the University

(5) The first of the Information Protection Principles in the PPIPA requires the University to limit its collection of personal information to that which is reasonably necessary to enable the University to fulfil its lawful purposes.

(6) The University was established by the Charles Sturt University Act 1989 (as amended) (the Charles Sturt University Act). The functions of the University, as stated in Section 7 of the Charles Sturt University Act, include:

a. the promotion, within the limits of the University's resources, of scholarship, research, free inquiry, the interaction of research and teaching, and academic excellence;
b. the provision of facilities for education and research of University standard, having particular regard to the needs and aspirations of the residents of western and south-western New South Wales;
c. the encouragement of the dissemination, advancement, development and application of knowledge informed by free inquiry;
d. the provision of courses of study or instruction across a range of fields, and the carrying out of research, to meet the needs of the community;
e. the participation in public discourse;
f. the conferring of degrees, including those of Bachelor, Master and Doctor, and the awarding of diplomas, certificates and other awards;
g. the provision of teaching and learning that engage with advanced knowledge and inquiry;
h. the development of governance, procedural rules, admission policies, financial arrangements and quality assurance processes that are underpinned by the values and goals referred to in the functions set out in this

subsection, and that are sufficient to ensure the integrity of the University's academic programs;

i. the exercise of commercial functions comprising the commercial exploitation or development, for the University's benefit, of any facility, resource or property of the University or in which the University has a right or interest (including, for example, study, research, knowledge and intellectual property and the practical application of study, research, knowledge and intellectual property), whether alone or with others;
j. the development and provision of cultural, sporting, professional, technical and vocational services to the community; and
k. such general and ancillary functions as may be necessary or convenient for enabling or assisting the University to promote the object and interests of the University, or as may complement or be incidental to the promotion of the object and interests of the University.

(7) The Act authorises the University to operate within or outside the State, including outside Australia.

Section 5 - Existing Laws and Policies

The Charles Sturt University Act and By-law

(8) The Charles Sturt University Act gives to the Council of the University the power to make by-laws. Neither the Charles Sturt University Act, nor the Charles Sturt University By-law 1995 (as amended) (the By-law) make any specific references to the collection, storage or use of personal information by the University.

Other Legislation

(9) The University is bound by legislation that protects peoples' privacy or controls the ways the University may deal with personal information. This legislation includes the Telecommunications (Interception) Act 1979 (Cth), the Listening Devices Act 1984 (NSW), the Criminal Records Act 1991 (NSW), the Workplace Video Surveillance Act 1998 (NSW), State Records Act 1998 (NSW) and the Health Records and Information PPIPA 2002 (NSW).

(10) The University is also bound to disclose personal information if required by the following legislation: the Higher Education Support Act 2003 (Clth); Higher Education Funding Act 1988 (Clth); Educational Services for Overseas Students Act 2000 (Clth); Higher Education Act 2001 (NSW); the Government Information (Public Access) Act 2009 (NSW); the Evidence Act 1995 (NSW); the Civil Procedures Act 2005 (NSW); the Independent Commission Against Corruption Act 1988, as well as comparable legislation and statutory instruments in other States and Territories in which the University operates or where claims may be validly lodged with a court or authority of competent jurisdiction; and various statutory instruments relating to professional registration, taxation, employment and superannuation.

Professional Codes of Practice

(11) Relevant University professional staff are bound by the codes of practice in respect of the confidentiality of the personal information they collect. These staff include psychologists and counsellors, health practitioners, ministers of religion and archivists. Universities Australia and the National Health and Medical Research Foundation have issued guidelines on ethics relating to research. Privacy is a major consideration in the guidelines. The Office of the Privacy Commissioner has issued Guides to Making Privacy Management Plans and Statutory Guidelines that have informed the development of this document.

University Policies

(12) In addition to its legislative obligations, the University has a number of policies that refer to the way personal information must be handled. These policies are identified below.

Code of Conduct (for all staff)

(13) The Code of Conduct specifies that "staff and students are entitled to confidentiality and privacy with respect to information which is personal to them. Staff have a duty to maintain the confidentiality, integrity and security of such information to which they have access in the normal course of their duties".

(14) With respect to the disclosure of information the Code requires that "Staff should only release information that they are authorised to release in the course of their duties" and "Staff should not release information in a manner which is misleading or which is likely to be misused".

Access to Personal Files (for staff)

(15) The Personal Files Access Policy sets out the rights of staff to access their personal file. Files may be perused in the offices of the Division of Human Resources and staff members may have notations added to their file providing comments or explanations with respect to any matters recorded on their file.

The Appointment of Agents and Representatives (by students)

(16) Clause 1 of the Student Appointment of Agents and Representatives Policy states "The University's dealings with a student are regarded by the University as private. The University shall not disclose its dealings with a student to any other persons or body without the student's permission except as required by law."

Access to Student Records (by students)

(17) The Access to Student Records and Assessment Items Policy informs students of their right to access their personal file and how they may exercise that right. This Policy stipulates that a student's academic record is regarded as confidential and will be released only to authorised University staff except where a student authorises otherwise. The Policy allows for the public release of academic assessments, including subject grades, assignment or test results; information on student demographics etc. but only in a way that prevents individual students from being identified. Refer to the Access to Student Records web page.

Exclusion Regulations

(18) A number of clauses in the Academic Progress Policy relate to the confidentiality of the records relating to the exclusion of students from courses, which often contain very private matters. Exclusion records are kept separate from a student's other records and the regulations allow for the suppression of details of particularly sensitive and distressing matters that contributed to a student's poor academic performance. The Exclusion penalty will be recorded, refer to the Academic Progress Regulations.

Use of Electronic Facilities (by staff and students)

(19) The Computing and Communications Facilities Use Policy applies to both students and staff, stipulates that users may only use the electronic facilities, files and information (which would include personal information) for University-related activities.

Records Management Policy

(20) The Records Management Policy reflects, among other things, the requirements of the PPIPA. One of the provisions of the Policy limits access to the personal records of staff, students and other clients of the University, to only those staff who need such access for the discharge of their duties.

Student Academic and General Misconduct

(21) The Student Academic Misconduct Policy and the Student General Misconduct Rule contain clauses governing the use of personal information that is used to establish whether a student is guilty of misconduct. The clauses require

such personal information to be filed separately from a student's other records and limits access to that information. The Penalty may be recorded. The Rules also stipulate that personal information collected with respect to an allegation of misconduct cannot be used for any other purpose unless agreed to by the student.

Section 6 - Information Protection Principles

(22) This section of the Plan details the extent to which the University complies with the Information Protection Principles.

Principle 1: Collection for Lawful Purposes

(23) The University's forms and websites used to collect personal information include a statement that explains the purpose for which the personal information is being collected. For students information is collected to assess applications for admission, management of their candidature and their relationship with the University and for Alumni relations. For staff information is collected for the management of their employment and their relationship with the University.

(24) A written statement is to be handed to students and staff or other clients seeking counselling or similar services within the University advising them that personal information will be collected as part of the service they are seeking and explaining to them the privacy obligations with which the University will comply in the use of that information. Where such personal information is also protected by a professional code of practice, advice is given to students and staff of that fact in the statement.

(25) A statement is issued to students who are to be audio or videotaped in the course of their studies that informs the students that if they agree to be recorded they are doing so of their own free will and tells them how the recordings will be used, stored, disclosed (or not) and disposed of and how they can gain access to the recording. Some lectures are recorded and the contribution of third parties may be also recorded during this process e.g. students asking questions or answering questions. In this instance recognition is made that these utterances may be covered by copyright and may contain visual images of the third party.

(26) 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. The University also invites students and the public to submit personal information online. These practices are not seen to be contrary to Information Protection Principle 1.

(27) Some groups' videotape or audiotape classes and use the tapes to provide feedback to students on their academic performance. All such taping is done with the knowledge and permission of the students involved and, therefore, is not in breach of the Information Protection Principles. However students are formally advised as to how the information will be used, stored, disclosed to others and disposed.

(28) The Division of Information Technology uses automated electronic systems to log the use by staff and students of the University's computer networks and systems. The Division uses this information from time to time as evidence in cases of alleged breaches of the Use of University Computing and Communications Facilities Policy . Staff are aware that a record is kept of their usage of the facilities for the sole purpose of monitoring their compliance with the Code as evidenced by an acknowledgment required each time their password is changed.

(29) The Talisma 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 seen to be contrary to Information Protection Principle 1.

Principle 2: Collection from the Person Concerned

(30) Most personal information collected by the University is collected directly from the person to whom it relates. Personal information relating to a prospective student's academic record may be obtained from other bodies, as consented to by the student signing a statement on the application form authorising the University to obtain such information if it is required. Similarly, personal information may be obtained from the referees of people seeking appointment as staff of the University or from staff seeking promotion. Again, the person's permission is obtained to do this.

(31) Some units obtain criminal record clearances from the NSW Police Service, or other relevant jurisdictions, on students and staff who are required to work with children. These clearances are authorised under the Child Protection (Prohibited Persons) Act 1998 (NSW) and the Commission for Children and Young People Act 1998 (NSW).

(32) The University sometimes collects from school children, who may be under 16 years of age, their name and address in order to mail to 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 quality assurance purposes. The University believes that this practice is not in breach of Information Protection Principle 2.

(33) The University may obtain the current contact details of graduates of the University from third parties without the graduates' knowledge or permission. The Office may use that information to make contact with those graduates to provide them with the opportunity to maintain contact with the University and access alumni services. Given that the intent of Information Protection Principle 2 is to prevent secret or undisclosed collections of personal information, it is the University's view that this does not breach the Principle.

(34) The University may obtain the current contact details of students of the University from third parties or applicants to the University without their knowledge or permission. The information to make contact with those persons to offer services of the University. Given that the intent of Information Protection Principle 2 is to prevent secret or undisclosed collections of personal information, it is the University view that such activities are not in breach of the Principle.

(35) Various units of the University concerned with investigating alleged breaches of the academic regulations or other rules of the University obtain personal information on people in the course of an investigation of misconduct from third parties without the permission of the parties to the matter. The information is made available to the parties, as required by the various rules and processes relating to alleged misconduct, who has the opportunity to respond. The University believes that the collection of personal information in these circumstances is covered by the exemption in section 24(4) of the PPIPA.

(36) Some units receive reports on students undertaking professional practice placements in schools, hospitals and other government and non-government organisations. Some of these supervisors would be regarded as adjunct staff of the University but some would not. Nevertheless, such 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.

Principle 3: Requirements for Collection

(37) The University's forms and websites used to collect personal information include a statement directing respondents to the University's Privacy Management Plan; the majority of units within the University either tell people at the time they collect personal information how that information will be used or they assert that the people providing the information could reasonably be expected to know why the information was being collected.

(38) Most units do not specifically advise people that they are being asked to provide information of their own free will but, again, assert that people could reasonably be expected to know that they were providing their personal information freely.

(39) The University does contract with outside organisations to use or store the personal information of its students or staff, and it does contract for the processing of some personal information. All such contracts identify that the entities will be bound by the same legislation as applicable to Charles Sturt University at any time.

(40) Some personal information relating to students is provided to outside organisations. For example, the DIISRTE is provided with personal information on students for the calculation of students' Higher Education Contribution Scheme (HECS) obligations, for statistical and planning purposes and to assess eligibility for Austudy and the Youth Allowance. Personal information is also provided to Unilinc for the purpose of registering students as users on this university libraries network. The personal information of overseas students studying in Australia is also sent to the Department of Immigration and Citizenship.

(41) Some personal information relating to staff is also made available to outside organisations but this is done only with the permission of the staff member. For example, salary details to the staff member's bank for the payment of salary and, for staff who travel on University business, certain personal information is supplied to corporate credit providers for travel card.

(42) The above disclosures are permitted under the PPIPA as they are made under statutory instruments and/or with the person's knowledge and permission.

Principle 4: Other Requirements for Collection

(43) Most personal information is provided to the University by the person to whom it relates and it is therefore assumed to be accurate. The Academic Regulations stipulate that students are responsible for the accuracy of their personal information and, through the University's website, are able and encouraged to amend their personal information as it changes. The Enrolment Wizard takes students through the Personal Details pages before moving into the subject enrolment pages and students are required to confirm their personal details at that stage of enrolment each year.

(44) Some personal information is verified before decisions based upon it are made. Such checks 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 personal information relevant to particular cases.

(45) Organisational units are to only collect personal information that is directly related to the work of their unit and, as a consequence, do not unreasonably intrude into people's personal affairs. In respect of students, the Exclusion and Special Consideration regulations allow for the details of particularly distressing or embarrassing matters that have adversely affected a student's performance to be suppressed. The University is more concerned to establish the effect particular circumstances had on a student and is less concerned with the details of those circumstances.

Principle 5: Retention and Security

(46) In late June 2000, State Records of New South Wales approved the General Disposal Authority: University Records (GDA9) . GDA9 imposes mandatory retention periods for the following records:

a. general administrative records (that are not adequately covered by other general disposal authorities issued by State Records);
b. student administration records; and
c. teaching and research records.

(47) The majority of 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. The Division is also responsible for ensuring that the University's electronic records are regularly backed-up and otherwise protected

against loss or damage.

(48) Protection against unauthorised access to, or modification or disclosure of, personal records held on the University's three primary systems (student, finance, personnel) is additionally controlled by security levels that control the functionality accorded to the various users of the systems.

Principle 6: Information about the Information Held

(49) Obtainable at the University Ombudsman's webpage.

Principle 7: Access to Information

(50) Procedures are in place that give students and staff access to their personal information at no cost and without excessive delay (refer clauses 15 and 17 of this Plan).

Principle 8: Alteration of Information

(51) The University encourages students or staff, as appropriate, to keep their personal information, particularly their contact details, up-to-date. The University's application for admission form includes a statement that identifies to students that information is managed under the requirements of the PPIPA and this includes the right to annotate and correct information held by the University.

Principle 9: Checking Information Before Use

(52) Much of the personal information collected by units either does not change or changes only occasionally (e.g. name, date of birth, marital status, gender, ethnicity). If such personal information does change and the change is not notified to the University, it is unlikely that the failure to notify would affect a decision taken by the University.

(53) 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, or fees, for which they are liable. Students must also check personal data at the time of on-line enrolment in subjects each teaching session in order to progress the enrolment process.

Principle 10: Limits on Use of Information

(54) The only units that use personal information, collected by the University, for purposes other than the purpose for which it was collected are the Division of Marketing and Communication's and Office of Governance and Corporate Affairs. These units use the personal information of students and prospective students for market research purposes, University promotion and alumni relations.

(55) Some units of the University use personal information, usually in aggregated format so that a particular person could not be identified, for quality assurance purposes. The University would contend that such a use of personal information would be for a purpose related to that for which the information was collected. That related purpose is to improve the quality of services provided to the University's clients.

Principle 11: Limits on Disclosure of Information

(56) Disclosures are limited by the statutory obligations of the University.

Principle 12: Special Restrictions on Disclosure

(57) Some units disclose personal information to bodies outside NSW, usually at the request of the person concerned. For example: for staff or students seeking positions in interstate or overseas organisations; and for students undertaking fieldwork placements interstate. The University also sends personal information relating to staff and

international students to affiliated institutions of the University that deliver the University's courses off-shore; this activity is deemed to be a routine management task for the University.

(58) The Division of 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 University is established under law to publicly examine students and to determine their competency for admission to a degree. As a certifying authority the decision of the University to award a qualification or degree is a public act and usually involves a public graduation ceremony and the printing of the names and qualifications of graduates in a handbook. The University is of the view that the award of qualifications is a public act and therefore verifying whether a person has obtained a particular qualification from the University, and their academic performance during their studies (i.e. their grades in a subject), for the purpose of determining the accuracy of the same is part of the legal obligations of the University and does not contravene the Information Privacy Principles.

Section 7 - Dealing with Privacy Concerns

Informal Reviews

(59) Staff, students and the public who 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 amended; or
d. express a concern about any of the above matters;

(60) are encouraged to contact the head of the organisational unit responsible for the personal information in question or the University Ombudsman.

(61) The handling of informal requests will be at no cost to the person seeking access to his/her personal information or a remedy.

(62) Where the University's informal review process is unable to resolve a privacy matter to the person's satisfaction, the person may lodge an application for an internal review with the University's Privacy Officer - currently the University Ombudsman.

Internal Reviews

(63) A person who is unhappy about the outcome of the informal process, or who chooses not to use it, may seek an internal review as provided by Part 5 of the PPIPA. The procedures as identified under Section 53 of the PPIPA will apply to Internal Reviews.

Section 8 - Training and Educational Strategy

(64) The obligations of the University as identified under the PPIPA will be the subject of information sessions conducted regularly by the University's Privacy Officer - currently the University Ombudsman. General alerts will also be made on University communication systems to remind staff and students of their privacy protection obligations. The University's Privacy Officer maintains a website for the University that provides more detailed information on privacy for those who need more, and/or ongoing, information about privacy issues.

Section 9 - Further Information

(65) People seeking further information or advice regarding the matters contained in this Plan should contact:

The University Ombudsman
Charles Sturt University
Locked Bag 588
Wagga Wagga NSW 2678

Telephone: 02 69334259
Email: ombudsman@csu.edu.au

Status and Details

Status	Historic
Effective Date	22nd May 2014
Review Date	31st May 2018
Approval Authority	Vice-Chancellor
Approval Date	11th May 2014
Expiry Date	25th September 2018
Unit Head	Cassandra Webeck University Secretary +61 2 6338 4258
Author	Col Sharp Director, Planning and Audit
Enquiries Contact	Lee Murrell University Ombudsman +61 2 6933 4254