Section 6 - Rules and Regulations

POLICY FOR THE USE OF UNIVERSITY COMPUTING AND COMMUNICATION FACILITIES

PART 1 - GENERAL

1. INTRODUCTION

1.1 The University provides an extensive range of computing and communication facilities for use by staff, students and other authorised users.

1.2 The conditions and obligations associated with authorised use of the University’s computing and communication facilities are set out in this policy.

1.3 This policy shall apply to all authorised users of University computing and communications facilities and applies to all of these facilities, irrespective of the Division, Faculty or other unit providing the facilities, and whether the facilities are located on a campus or site of the University or elsewhere.

1.4 This policy shall operate in conjunction with:
   (i) The 'Charles Sturt University web Policy' as approved by Academic Senate. This policy regulates publication of all materials mounted on a web server of Charles Sturt University;
   (ii) The Charles Sturt University 'Policy on the Allowed Access to CSUNet'. This policy sets out Charles Sturt University’s corporate responsibilities and obligations in regards to its communications and network infrastructure;
   (iii) The Charles Sturt University 'Mobile Telephone Policy'. This policy sets out the procedures for the purchase and charging of mobile telephones used for official purposes by employees of Charles Sturt University;
   (iv) The Charles Sturt University 'Code of Conduct for Staff'. This Code aims to foster and maintain public trust and confidence in the integrity and professionalism of the staff of the University;
   (v) The Charles Sturt University 'Student General Misconduct Rule'; and
   (vi) The Charles Sturt University 'Academic Misconduct Rule'.

2. OBJECTIVES

2.1 The objectives of this policy are to:

2.1.1 facilitate the efficient, effective, responsible and lawful use of the University’s computing and communication facilities;

2.1.2 safeguard the interests of the University and all authorised users of the University’s computing and communication facilities; and

2.1.3 provide guidelines and instructions to authorised users in the appropriate use of the University’s computing and communication facilities.

3. NETWORK SECURITY

3.1 The maintenance and enhancement of the security and integrity of the University’s computing and communication network is essential to fulfilment of the University’s mission and corporate obligations and responsibilities.

3.2 The University reserves the right to implement all appropriate measures to manage its computing and communication facilities in an efficient and effective manner and to maintain and enhance the security of its computing and communications network.

3.3 In particular, the Executive Director, Division of Information Technology (or nominee) is authorised to develop and implement procedures and technologies to:
   (i) audit and to monitor the usage of any or all of the University’s computing and communication network and facilities, to ensure that these facilities are used and managed in a secure, efficient and effective manner;
   (ii) deal with existing or potential threats to the security and integrity of the University’s computing and communication network;
   (iii) prevent unauthorised access to and usage of the University’s computing and communication network and facilities;
   (iv) restrict the use of any University computer or communication facility that impedes the secure or efficient operation of the University’s network;
   (v) remove or delete without notice any data, material or software that presents a risk to the security or integrity of the University’s network or computing or communication facilities;
   (vi) delete non-registered servers from the University network; and
   (vii) maintain the integrity of material mounted on the University’s website, including the publication of authorised information relating to the official business of the University.

4. DEFINITIONS

Authorised User shall mean and refer to:
   (i) an employee of the University;
   (ii) a student of the University;
   (iii) a person who holds an honorary or visiting appointment;
   (iv) a Student or Staff Association;
   (v) an entity wholly owned by the University;
   (vi) a participant in a Collaborative Research Centre, Co-operative Multimedia Centre and other collaborative ventures where the
principal objective of such a collaborative venture is the advancement of University teaching, administration and/or research;
(vii) a publicly funded not-for-profit research agency that jointly undertakes teaching, administration and/or research programs with the University;
(viii) a participant in a conference, congress or workshop where an educational, research or professional society association with the University exists but not where a conference, congress or workshop has a primary commercial purpose or objective; and
(ix) any other person approved by the Executive Director, Information Technology as an authorised user e.g. a member of the University Council.

Communication facilities include, but are not restricted to, the following items:
(i) E-mail;
(ii) Facsimiles;
(iii) Internet;
(iv) Pagers;
(v) Satellite communications equipment;
(vi) Telephones: landline and mobile; and
(vii) Two way radios.

Computing facilities include, but are not restricted to, the following items:
(i) Computer hardware, free-standing computers, networked computers, time shared computers, terminals;
(ii) Peripherals such as printers, scanners, electronic cameras or mobile telephones connected to the network;
(iii) Media, CD Roms and disks;
(iv) Computer software;
(v) Network connections;
(vi) Operating and user manuals; and
(vii) Video conferencing systems.

Employee shall mean and refer to any staff member of the University, including a person employed by the University on a casual basis.

Prohibited data or material shall mean and refer to all data or material that falls within the categories described in points (i) to (v) below, and as proscribed or defined within relevant Commonwealth and State legislation:
(i) describes, depicts, express or otherwise matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of decency and propriety generally accepted by reasonable adults;
(ii) describes or depicts in a way that is likely to cause offence to a reasonable adult, a minor who is, or who appears to be, under 16 years of age whether the minor is engaged in sexual activity or not;
(iii) promotes, incites or instructs in matters of crime or violence;
(iv) discriminates against, harasses or viliﬁes any member of the public on the grounds of sex, pregnancy, age, race, nationality, descent or ethnic background, religious background, marital status, disability, HIV/AIDS, sexual preference, homosexuality and transgender; or
(v) defames or could be reasonably anticipated to defame, any person, institution or company.

Student shall mean and refer to a person enrolled in:
(i) a course leading to an award of the University; or
(ii) a course not leading to an award of the University but which comprises subjects drawn from a course or courses leading to an award or awards of the University.

5. DISCLAIMER
5.1 The University shall make available to employees, students and other authorised users a range of computing and communication facilities. The University accepts no responsibility for any damage to or loss of data arising directly or indirectly from use of these facilities or for any consequential loss or damage. The University makes no warranty, express or implied, regarding the computing and communication facilities offered, or their fitness for any particular purpose.

5.2 Whilst reasonable care is taken, the University cannot guarantee the confidentiality of any data stored on any University computer system or transmitted through any network.

5.3 The University’s liability in the event of any loss or damage shall be limited to any fees and charges paid to the University for the use of the computing facilities that resulted in the loss or damage.

PART 2 - PROVISIONS FOR USE BY ALL AUTHORISED USERS
6. PROHIBITED USE OF COMPUTER AND COMMUNICATION DEVICES
6.1 The use of any University computer or communications facility to make, send or store fraudulent, unlawful, harassing or abusive calls or messages is prohibited.

6.2 The use of any University computer or communications facility that impedes the efficient and effective operation of such facilities is
Policy for the Use of University Computing and Communication Facilities

prohibited (e.g. unauthorised bulk or all user and chain letter e-mails).

6.3 An authorised user shall not use any University computer or communications facility to access, transfer, publish, display, circulate or store prohibited material, messages or data as defined in clause 4 - Definitions of this policy.

6.4 The prohibitions contained within subclause 6.3 shall not apply where an authorised user is engaged in a responsible and honest search of a valid academic or research purpose.

6.5 The University reserves the right to audit and to remove without notice any fraudulent, unlawful or prohibited data or material from its computing or communications facilities.

6.6 An employee, student or other authorised user who receives any threatening intimidating or harassing telephone call or electronic message may report the incident to the Executive Director, Information Technology (or nominee) in the first instance.

6.7 An employee, student or other authorised user who becomes aware of a breach of this policy may report the matter to the Executive Director, Information Technology (or nominee) in the first instance.

7. LOGIN IDENTIFICATION

7.1 An authorised user shall not:
(i) disclose his or her login identification to any other party or parties;
(ii) allow another party to use his or her login identification;
(iii) use the login identification of another user;
(iv) attempt to discover any other user's login identification; and
(v) take every reasonable precaution to ensure that his or her login identification is adequately secured.

7.2 The provisions of subclause 7.1 (i) to (iv) shall not apply:
(i) to those persons authorised by the Executive Director, Division of Information Technology (or nominee) to carry out any of these acts in the performance of duties directly related to their work; or
(ii) where an authorised user is requested to carry out any of these acts by a person authorised by the Executive Director, Division of Information Technology (or nominee).

7.3 Where an authorised user becomes aware that the security of their logon identification has been breached the matter should be reported without delay in the first instance to the Executive Director, Information Technology.

8. SECURITY

8.1 An authorised user shall not infringe the University's security system or use University computing or communications facilities to breach the security of systems accessible via the networks provided by the University.

8.2 An authorised user shall not introduce virus software or any other software designed to disrupt, corrupt or destroy programs and/or data, or sabotage the University's computing and communication facilities.

8.3 An authorised user shall not, without the written authorisation of the Executive Director, Information Technology:
(i) examine, copy, rename, change or delete programs, files, data, messages or information belonging to the University or any other authorised user;
(ii) use the University's computing or communication facilities for profit making or commercial activities;
(iii) modify any equipment or software; or
(iv) alter any restrictions associated with any University computer system, computer account, network system, personal computer software protection or other of the University's computing or communication facilities.

8.4 The provisions of subclause 8.3 (i) to (iv) shall not apply where an authorised user is required to carry out any of these acts in the performance of duties directly related to their work or, in the case of students, to their academic program.

9. BULK E-MAIL MESSAGES

9.1 Distribution of bulk e-mail messages (all system users' e-mail) on the University e-mail system by an authorised user requires the authorisation of the Executive Director, Information Technology (or nominee) or Vice-Chancellor, and shall only be permitted in emergency situations where the existing University-wide information services are considered to be inappropriate or inadequate.

10. COPYRIGHT

10.1 An authorised user shall be personally responsible for complying with relevant provisions of the Copyright Act 1968 (Cth), as amended, particularly as it relates to the copying and communication of computer software and other copyright material on the internet.
4 - Rules and Regulations

10.2 An authorised user should consult the University’s copyright website (www.csu.edu.au/copyright/) for further information concerning copyright restrictions and obligations or contact their campus library.

PART 3 - OBLIGATIONS OF EMPLOYEES

11. OBLIGATIONS

11.1 In addition to the conditions and privileges of use set out in Parts 1 and 2 of this policy, all employees are obliged to ensure that:
(i) the use of University computing and communication facilities is directed toward achievement of the academic and administrative goals of the University;
(ii) University computing and communication facilities are used in a manner which is lawful, efficient, proper and ethical;
(iii) University computing and communication facilities are used to carry out job related tasks in an economical manner; and
(iv) the express provisions of usage as set out in this part of the policy are adhered to at all times.

11.2 To assist in fulfilling the obligations set out above at subclause 11.1, the University reserves the right to audit and to monitor the use by employees of the University’s computing and communication network and facilities.

12. PRIVATE USE OF UNIVERSITY COMPUTING AND COMMUNICATIONS FACILITIES

12.1 The University aims to enhance the quality of the working life of its employees and to retain skilled and experienced employees by providing flexibility in employment practices and work arrangements. As a consequence of this approach, the University will allow as a privilege, reasonable use of University computing and communications facilities for private purposes.

12.2 An employee shall not use University computing and communications facilities for any purpose that is questionable, controversial or offensive specifically including the following activities:
(i) gambling;
(ii) transferral, publication, display or circulation of chain letters or junk mail;
(iii) accessing chat lines;
(iv) downloading of unauthorised software;
(v) downloading of lengthy files containing picture images, live pictures or graphics;
(vi) accessing computer games or radio or television stations broadcasting via the internet; or
(vii) accessing or transmitting prohibited data or material.

12.3 The prohibitions contained in subclause 12.2 (iii), (v), (vi) and (vii) shall not apply where an employee is required to carry out such activities in the performance of his or her official duties.

13. MOBILE TELEPHONES USED FOR OFFICIAL PURPOSES

13.1 The Vice-Chancellor (or nominee) may authorise the allocation to an employee of a University owned mobile telephone in the following circumstances:
(i) where an employee is required in the performance of his or her official duties to:
(a) monitor University equipment and services outside normal working hours;
(b) attend to an emergency or breakdown on the premises of the University;
(c) be available to respond and attend expeditiously to a critical incident or urgent problem (e.g. UAC rounds, a major machine replacement or a potential emergency on the premises of the University); or
(d) in the case of DIT employees, to answer and respond to telephone calls for support from authorised users and to take action as appropriate, such as assessing requests, providing advice to these authorised users, taking immediate remedial action or contacting the appropriate person to take such action; or
(ii) where the Vice-Chancellor (or nominee) is satisfied that the duties and responsibilities of a position to which an employee is appointed warrant the allocation of a University owned mobile telephone.

13.2 The University’s ‘Mobile Telephone Policy’ sets out the delegations and procedures for the acquisition by an employee of a University-owned mobile telephone. In addition to the provisions of the University’s ‘Mobile Telephone Policy’, an employee who has acquired a University owned mobile telephone is required to:
(i) ensure that precautions are taken to secure the mobile telephone against theft or damage;
(ii) keep the duration of all calls made from the mobile telephone to the minimum time necessary; and
(iii) be accountable for all calls made from the mobile telephone.

14. CONFIDENTIALITY AND PRIVACY

14.1 Employees must be aware that the confidentiality of electronic communications cannot be assured and that:
(i) all data or messages transmitted by electronic communications facilities are capable of being intercepted, traced or recorded by others; and
(ii) all electronic messages are official documents subject to the same laws that govern all other forms of correspondence.

14.2 An employee shall familiarise him or her self with:
(i) the individual and institutional responsibilities that relate to their job and the protection of confidential or sensitive information; and
(ii) the statutory responsibilities that relate to their job and the protection of information deemed to be 'personal information' by the Privacy and Personal Information Protection Act 1998 (NSW).

14.3 An employee shall be required to comply with relevant statutory requirements, including the provisions of the Privacy and Personal Information Protection Act 1998 (NSW) and the University's 'Privacy Management Plan'.

14.4 An employee shall not breach obligations that relate to the protection of confidential or sensitive information and information deemed to be 'personal information' by the Privacy and Personal Information Protection Act 1998 (NSW).

15. RECORD KEEPING
15.1 All electronic business communications are official University records and subject to the same standards of record keeping that apply to 'paper' records.

15.2 An employee shall familiarise him or her self with all individual and institutional responsibilities that relate to their job and to applicable record keeping standards.

15.3 An employee shall not breach obligations that relate to applicable standards of record keeping.

PART 4 - OBLIGATIONS OF STUDENTS
16. OBLIGATIONS
16.1 In addition to the conditions of use set out in Parts 1 and 2 of this policy, all students shall be accountable for the particular obligations as set out in Part 4 of this policy.

16.2 Subject to the provisions of subclause 16.3, a student shall only use University computing and communication facilities for University and course-related activities.

16.3 The University will allow, as a privilege to students, limited use of the University’s e-mail system for private purposes, provided that such e-mails do not:
(i) contain or link to prohibited or unlawful data or material; or
(ii) support the operation of a non-University related business, enterprise or activity.

16.4 A student shall not:
(i) access or transmit prohibited or unlawful data or material;
(ii) obtain or attempt to obtain a higher than authorised level of privilege on any University computing or communication facility;
(iii) abuse, remove or tamper with any of the computing or communication facilities provided by the University;
(iv) store data in an area unauthorised for such storage;
(v) collect or discard the output from the University’s computing or communication facilities of any other authorised user;
(vi) work in a way that distracts or harasses any other authorised user or member of the public; or
(vii) remove, deface or corrupt notices placed by an employee of the University regarding the use of University computing or communication facilities.

17. CONFIDENTIALITY
17.1 Students must be aware that the confidentiality of electronic communications cannot be assured and that all data or messages transmitted by electronic communications facilities are capable of being intercepted, traced or recorded by others.

17.2 The University reserves the right to audit and to monitor the use of University computing and communications facilities.

PART 5 - OBLIGATIONS OF AUTHORISED USERS OTHER THAN EMPLOYEES AND STUDENTS
18. OBLIGATIONS
18.1 In addition to the conditions of use set out in Parts 1 and 2 of this policy, all authorised users other than employees and students shall be accountable for the particular obligations as set out in Part 5 of this policy.

18.2 Subject to the provisions of subclause 18.3, an authorised user shall only use University computing and communication facilities:
(i) for the purpose of fulfilling administrative, teaching, research or academic related requirements; and
(ii) in a manner that is lawful, efficient, proper and ethical.

18.3 The University will allow, as a privilege to authorised users, limited use of the University’s e-mail system for private purposes, provided that such e-mails do not:
6 - Rules and Regulations

(i) contain or link to prohibited or unlawful data or material; or
(ii) support the operation of a non-University related business, enterprise or activity.

18.4 An authorised user shall not:
(i) access or transmit prohibited or unlawful data or material;
(ii) obtain or attempt to obtain a higher than authorised level of privilege on any University computing or communication facility;
(iii) abuse, remove or tamper with any of the computing or communication facilities provided by the University;
(iv) collect or discard the output from the University's computing or communication facilities of any other authorised user;
(vi) work in a way that distracts any other authorised user; or
(vii) remove, deface or corrupt notices placed by an employee of the University regarding the use of University computing or communication facilities.

19. CONFIDENTIALITY

19.1 Authorised users must be aware that the confidentiality of electronic communications cannot be assured and that all data or messages transmitted by electronic communications facilities are capable of being intercepted, traced or recorded by others.

19.2 The University reserves the right to audit and to monitor the use of University computing and communications facilities.

PART 6 - BREACH OF POLICY

20. EMPLOYEES

20.1 An employee who is alleged to have breached the provisions of this policy may be subject to disciplinary action under the applicable industrial award or agreement.

20.2 In accordance with the provisions of the applicable industrial award or agreement, an employee who is found to have breached the provisions of this policy may be subject to one of the following actions:
(i) counselling;
(ii) formal censure;
(iii) withholding of a salary step or point;
(iv) demotion by one or more salary steps or points;
(v) demotion by one or more classification levels; or
(vi) termination of employment.

21. STUDENTS

21.1 Where the Executive Director, Division of Information Technology (or nominee), is of the opinion that a student has breached the provisions of this policy and that the breach amounts to misconduct, or that there is an imminent threat of misconduct by the student, the Executive Director Division of Information Technology (or nominee) may suspend the student's access to University computing and communication facilities for a period of up to two weeks.

21.2 In accordance with the provisions of the Student General Misconduct Rule or any other relevant student misconduct provisions, a student who is found to have breached the provisions of this policy may be subject to one or more of the following actions:
(i) caution or reprimand;
(ii) demand for payment of expenses incurred by the student, or damage sustained by the University;
(iii) imposition of a fine;
(iv) suspension from the use of any University facility, or entrance to University owned property; and/or
(v) suspension from the University.

22. ALL AUTHORISED USERS OTHER THAN EMPLOYEES OR STUDENTS

Any authorised user, other than an employee or student, who is found by the Vice-Chancellor (or nominee) to have breached the provisions of this policy may be subject to:
(i) termination or suspension of their access to University computer or communication facilities;
(ii) reimbursement of expenses incurred; and/or
(iii) any other such action that the Vice-Chancellor may deem appropriate.

23. REPORTING OF BREACH

The University reserves the right to report any breach of this policy that may require investigation to the police or any other appropriate authority external to the University.