



Title:

Policy for the Use of University Computing and Communication Facilities

Version	3.0
TRIM file number	06/275
Short description	A policy on the authorised use of CSU's computing and communication facilities
Relevant to	All employees
Approved by	Executive Committee of Council
Responsible officer	Executive Director, Human Resources
Responsible office	Division of Human Resources
Date introduced	16 August, 2001 (PER12 – resolution CNL01/156)
Date(s) modified	17 October, 2001 (resolution CNL01/183) 18 November, 2005 (resolution EXE 05/106) 18 August 2006 (resolution EXE 06/64) 27 October 2008 3 December 2008 20 July 2009
Next scheduled review date	October, 2010
Related University documents	Charles Sturt University Web Policy Policy on the Allowed Access to CSUNet Mobile Telephone Policy Code of Conduct for Staff Student General Misconduct Rule Academic Misconduct Rule
Related legislation	
Key words	policy, computing, computer use, electronic communication, e-mail, Internet, network, telephones

PART 1 - GENERAL

1. PURPOSE

- 1.1 Charles Sturt University (CSU) 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 CSU's computing and communication facilities are set out in this policy.
- 1.3 The objectives of this policy are to:
 - (a) facilitate the efficient, effective, responsible and lawful use of CSU's computing and communication facilities;
 - (b) safeguard the interests of CSU and all authorised users of its computing and communication facilities; and
 - (c) provide guidelines and instructions to authorised users in the appropriate use of CSU's computing and communication facilities.

2. SCOPE

This policy applies to all authorised users of CSU's computing and communications facilities, irrespective of the Division, Faculty or other unit providing the facilities, and whether the facilities are located on a campus or site of CSU or elsewhere.

3. REFERENCES

This policy shall operate in conjunction with:

- (a) 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;
- (b) The Division of Information Technology Privacy Statement, detailing what personal information is stored, and how or why it is used;
- (c) The Charles Sturt University "Policy on the Allowed Access to CSUNet". This policy sets out CSU's corporate responsibilities and obligations in regards to its communications and network infrastructure;
- (d) CSU Records Management Policy;
- (e) 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 CSU;
- (f) 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 CSU;

- (g) The Charles Sturt University "Student General Misconduct Rule"; and
- (h) The Charles Sturt University "Academic Misconduct Rule";
- (i) The Spam Act 2003;
- (j) The Telecommunications Act 1997.

4. DEFINITIONS

4.1 **Authorised user** means and refers to:

- (a) an employee of CSU;
- (b) a student of CSU;
- (c) a person who holds an honorary or visiting appointment;
- (d) any external organisation or person that has a commercial arrangement with CSU;
- (e) an entity wholly owned by CSU;
- (f) a participant in a Collaborative Research Centre, Co-operative Multimedia Centre and other collaborative ventures where the principal objective is the advancement of University teaching, administration and/or research;
- (g) a publicly funded, not-for-profit research agency that jointly undertakes teaching, administration and/or research programs with CSU;
- (h) a participant in a conference, congress or workshop where an educational, research or professional society association with CSU exists but not where a conference, congress or workshop has a primary commercial purpose or objective; and
- (i) any other person approved by the Executive Director, Information Technology (or nominee) as an authorised user, e.g. a member of the University Council.

4.2 **Communication facilities** include, but are not restricted to, the following items:

- (a) e-mail;
- (b) facsimiles;
- (c) Internet;
- (d) pagers;

- (e) satellite communications equipment;
- (f) telephones: landline and mobile;
- (g) two-way radios;
- (h) forums, blogs, wikis podcasts, vodcasts and other internet based communications tools.

4.3 Computing facilities include, but are not restricted to, the following items:

- (a) computer hardware, desktop and laptop computers, computer terminals, er mobile phones and other portable computing devices
- (b) peripherals such as printers, scanners, digital cameras
- (c) media, CD-ROMs, DVDs, Blu-Rays, disks and memory storage devices;
- (d) computer software and firmware;
- (e) network connections (both wired and wireless);
- (f) operating and user manuals; and
- (g) video conferencing and other presence technologies.

4.4 Employee means and refers to any staff member of CSU, including a person employed by CSU on a casual basis.

4.5 Prohibited data or material means and refers to all data or material that falls within the categories described in points (a) to (e) below, and as prohibited or defined within relevant Commonwealth and State legislation:

- (a) describes or depicts, expressly 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;
- (b) describes or depicts a minor who is, or who appears to be, under 16 years of age, whether the minor is engaged in sexual activity or not, in a way that is likely to cause offence to a reasonable adult;
- (c) promotes, incites or instructs in matters of crime or violence;
- (d) 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
- (e) defames or could be reasonably anticipated to defame, any person, institution or company.

4.6 Student means and refers to a person enrolled in:

- (a) a course leading to an award of CSU; or
- (b) a course not leading to an award of CSU but comprising subjects drawn from a course or courses leading to an award or awards of CSU.

5. NETWORK SECURITY

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

5.2 CSU 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.

5.3 In particular, the Executive Director, Information Technology (or nominee) is authorised to develop and implement procedures and technologies to:

- (a) audit and monitor the usage of any or all of CSU's computing and communication network and facilities, to ensure that these facilities are used and managed in a secure, efficient and effective manner;
- (b) deal with existing or potential threats to the security and integrity of CSU's computing and communication network;
- (c) prevent unauthorised access to and usage of CSU's computing and communication network and facilities;
- (d) restrict the use of any CSU computer or communication facility that impedes the secure or efficient operation of CSU's network;
- (e) remove or delete without notice any data, material or software that presents a risk to the security or integrity of CSU's network or computing or communication facilities;
- (f) Remove or disable access to unauthorised equipment from CSU's network
- (g) maintain the integrity of material mounted on CSU's website, including the publication of authorised information relating to the official business of CSU.
- (h) remove or delete without notice any data, material or software that is in breach of copyright legislation.

6. DISCLAIMER

- 6.1 CSU shall make available a range of computing and communication facilities to employees, students and other authorised users. CSU 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. CSU makes no warranty, express or implied, regarding the computing and communication facilities offered, or their fitness for any particular purpose.
- 6.2 Whilst reasonable care is taken, CSU cannot guarantee the confidentiality of any data stored on any CSU computer system or transmitted through any network.
- 6.3 CSU's liability in the event of any loss or damage shall be limited to any fees and charges paid to CSU for the use of the computing facilities that resulted in the loss or damage.

PART 2 - PROVISIONS FOR USE BY ALL AUTHORISED USERS

7. PROHIBITED USE OF COMPUTER AND COMMUNICATION DEVICES

- 7.1 The use of any CSU computer or communications facility to make, send or store fraudulent, unlawful, harassing or abusive calls or messages is prohibited.
- 7.2 The use of any CSU computer or communications facility that impedes the efficient and effective operation of such facilities is prohibited (e.g. unauthorised bulk, spam or all user e-mails).
- 7.3 An authorised user shall not use any CSU computer or communications facility to access, transfer, publish, display, circulate or store prohibited material, messages or data as defined in sub-clause 4.5 of this policy.
- 7.4 The prohibitions contained within subclause 7.3 shall not apply where an authorised user is engaged in a responsible and honest search for a valid academic or research purpose.
- 7.5 CSU reserves the right to audit and remove without notice any fraudulent, unlawful or prohibited data or material from its computing or communications facilities.
- 7.6 An employee, student or other authorised user who receives any threatening, intimidating or harassing telephone call or electronic message should report the incident to the Executive Director, Information Technology (or nominee) in the first instance.
- 7.7 An employee, student or other authorised user who becomes aware of a breach of this policy should report the matter to the Executive Director, Information Technology (or nominee) in the first instance.

8. LOGIN IDENTIFICATION

- 8.1 An authorised user shall:
 - (a) not disclose his or her login identification to any other party or parties;
 - (b) not allow another party to use his or her login identification;
 - (c) not use the login identification of another user;
 - (d) not attempt to discover any other user's login identification; and
 - (e) take every reasonable precaution to ensure that his or her login identification is adequately secured.
- 8.2 The provisions of subclause 8.1 (a) to (e) shall not apply:

- (a) to those persons authorised by the Executive Director, Information Technology (or nominee) to carry out any of these acts in the performance of duties directly related to their work; or
 - (b) where an authorised user is requested to carry out any of these acts by a person authorised by the Executive Director, Information Technology (or nominee).
- 8.3 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 (or nominee).

9. SECURITY

- 9.1 An authorised user shall not infringe CSU's security system or use CSU computing or communications facilities to breach the security of systems accessible via the networks provided by CSU.
- 9.2 An authorised user shall not introduce virus software or any other software or technology designed to disrupt, corrupt or destroy programs and/or data, or sabotage CSU's computing and communication facilities.
- 9.3 An authorised user shall not, without the written authorisation of the Executive Director, Information Technology:
- (a) examine, copy, rename, change or delete programs, files, data, messages or information belonging to CSU or any other authorised user;
 - (b) use CSU's computing or communication facilities for profit-making or commercial activities;
 - (c) modify any hardware or software; or
 - (d) alter any restrictions associated with any CSU computer system, computer account, network system, personal computer software protection or other of CSU's computing or communication facilities.
- 9.4 The provisions of subclause 9.3 (a) to (d) 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.

10. SPAM and BULK E-MAIL MESSAGES

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

11. COPYRIGHT

- 11.1 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.
- 11.2 An authorised user should consult CSU's copyright website (www.csu.edu.au/copyright/) for further information concerning copyright restrictions and obligations or contact their campus library.

12. CONFIDENTIALITY

- 12.1 Authorised users must be aware that the confidentiality of electronic communications cannot be assured and that all data or messages transmitted by electronic communication facilities are capable of being intercepted, traced or recorded by others.
- 12.2 CSU reserves the right to monitor and audit the use by authorised users of CSU's computing and communication network and facilities and conduct an investigation where it has reasonable grounds that a breach of this policy has occurred.
- 12.3 An investigation may include (but not be limited to) investigations into:
- (a) Email use
 - (b) Internet use
 - (c) Storage of data on desktop and laptop computers
 - (d) Storage of data on shared network services
 - (e) Telephone usage
 - (f) Mobile phone usage
- 12.4 Investigations are conducted after receiving the permission of the Executive Director, Information Technology (or nominee), and take into account privacy implications and with direction to the underlying reason for the investigative audit.
- 12.5 The University reserves the right to permit a staff member to access potentially personal and/or confidential information in the following circumstances:
- (a) Where a technical fault or error has occurred or has been reported and access is necessary in the course of identifying and rectifying the fault.
 - (b) Where access is required for the University to continue its business and the owner or creator of the information is unavailable or cannot provide access.

PART 3 - OBLIGATIONS OF EMPLOYEES

13. OBLIGATIONS

13.1 In addition to the conditions and privileges of use set out in Parts 1 and 2 of this policy, all employees shall ensure that:

- (a) the use of CSU computing and communication facilities is directed toward achievement of the academic and administrative goals of CSU;
- (b) CSU computing and communication facilities are used in a manner which is lawful, efficient, proper and ethical;
- (c) CSU computing and communication facilities are used to carry out job related tasks in an economical manner; and
- (d) the provisions of usage as set out in this part of the policy are adhered to at all times.

13.2 A employee shall not:

- (a) access or transmit prohibited or unlawful data or material;
- (b) obtain or attempt to obtain a higher than authorised level of privilege on any CSU computing or communication facility;
- (c) abuse, remove or tamper with any of the computing or communication facilities provided by CSU;
- (d) work in a way that distracts, defames or harasses any other authorised user or member of the public;
- (e) use the CSU computing system to support the operation of a non-CSU related business, enterprise or activity;
- (f) use the CSU computing system to store, transfer or reproduce copyrighted material.

14. PRIVATE USE OF UNIVERSITY COMPUTING AND COMMUNICATIONS FACILITIES

14.1 CSU 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. Consequently, CSU will allow, as a privilege, reasonable use of CSU computing and communications facilities for personal purposes where such use has no negative impact on the performance of that employee in the performance of their duties or adverse impact on CSU information technology facilities

14.2 An employee shall not use CSU computing and communications facilities for any purpose that is questionable, controversial or offensive, specifically including, but not limited to:

- (a) gambling;
- (b) transferral, publication, display or circulation of spam or junk mail;
- (e) downloading or uploading files with prohibited, inappropriate or illegal content including that which infringes copyright
- (f) excessively accessing online content via the Internet such as computer games, video and audio content streaming, online messaging and chat.
- (g) accessing or transmitting prohibited data or material.

14.3 The prohibitions contained in subclause 13.2 (e), (f) and (g) shall not apply where an employee is required to carry out such activities in the performance of his or her official duties.

14.4 Where a Manager or Supervisor has reasonable grounds to believe that an employee is in breach of these conditions they may request an investigation into such access and if proven valid may revoke these privileges.

14.5 In circumstances where upon investigation, it has been found that the use of Computing and Communications facilities for personal use has been excessive, the University may request compensation for such access.

- (a) With regard to internet access, data downloads greater than 1 gigabyte per month would be considered excessive.

15. MOBILE PHONES USED FOR OFFICIAL PURPOSES

15.1 The Dean or Executive Director may authorise the allocation to an employee of a University owned mobile telephone in the following circumstances:

- (a) where an employee is required in the performance of his or her official duties to:
 - monitor CSU equipment and services outside normal working hours;
 - attend to an emergency or breakdown on the premises of CSU;
 - be available to respond and attend quickly to a critical incident or urgent problem (e.g. UAC rounds, a major machine replacement or a potential emergency on the premises of CSU); or
 - in the case of Division of Information Technology (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

- (b) where the Dean or Executive Director 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.

15.2 CSU's "Mobile Phone Policy" sets out the delegations and procedures for the acquisition of a University owned mobile telephone by an employee. In addition to the provisions of CSU's "Mobile Telephone Policy", an employee who has acquired a University owned mobile telephone shall:

- (a) ensure that precautions are taken to secure the mobile telephone against theft or damage;
- (b) keep the duration of all calls made from the mobile telephone to the minimum time necessary; and
- (c) be accountable for all calls made from the mobile telephone.

16. CONFIDENTIALITY AND PRIVACY

16.1 Employees must be aware that the confidentiality of electronic communications cannot be assured and that:

- (a) all data or messages transmitted by electronic communication facilities are capable of being intercepted, traced or recorded by others; and
- (b) all electronic messages are official documents subject to the same laws that govern all other forms of correspondence.

16.2 An employee shall familiarise him or herself with:

- (a) the individual and institutional responsibilities that relate to his or her job and the protection of confidential or sensitive information; and
- (b) the statutory responsibilities that relate to his or her job and the protection of information deemed to be "personal information" by the *Privacy and Personal Information Protection Act 1998 (NSW)*.

16.3 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 CSU's "Privacy Management Plan".

16.4 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)*.

17. RECORD KEEPING

- 17.1 All electronic business communications are official CSU records and subject to the same standards of record keeping that apply to "paper" records.
- 17.2 An employee shall familiarise him or herself with all individual and institutional responsibilities that relate to his or her job and to applicable record keeping standards.
- 17.3 An employee shall not breach obligations that relate to applicable standards of record keeping.

PART 4 - OBLIGATIONS OF STUDENTS

18. OBLIGATIONS

18.1 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 .

18.2 A student shall not:

- (a) access or transmit prohibited or unlawful data or material;
- (b) obtain or attempt to obtain a higher than authorised level of privilege on any CSU computing or communication facility;
- (c) abuse, remove or tamper with any of the computing or communication facilities provided by CSU;
- (d) store data in an area unauthorised for such storage;
- (e) collect or discard the output of any other authorised user from CSU's computing or communication facilities;
- (f) work in a way that distracts, defames or harasses any other authorised user or member of the public;
- (g) remove, deface or corrupt notices placed by a CSU employee regarding the use of CSU computing or communication facilities;
- (h) use the CSU computing system to support the operation of a non-CSU related business, enterprise or activity;
- (i) use the CSU computing system to store, transfer or reproduce copyrighted material.

PART 5 - OBLIGATIONS OF AUTHORISED USERS OTHER THAN EMPLOYEES AND STUDENTS

19. OBLIGATIONS

19.1 In addition to the conditions of use set out in Parts 1 and 2 of this policy, all 'other' authorised users other than employees and students shall be accountable for the particular obligations as set out in Part 5 of this policy .

19.2 Subject to the provisions of subclause 19.3, 'other' authorised users shall only use CSU computing and communication facilities:

- (a) for the purpose of fulfilling administrative, teaching, research or academic related requirements; and
- (b) in a manner that is lawful, efficient, proper and ethical.

19.3 An 'other' authorised user shall not:

- (a) access or transmit prohibited or unlawful data or material;
- (b) obtain or attempt to obtain a higher than authorised level of privilege on any CSU computing or communication facility;
- (c) abuse, remove or tamper with any of the computing or communication facilities provided by CSU;
- (d) store data in an area unauthorised for such storage;
- (e) collect or discard the output of any other authorised user from CSU's computing or communication facilities;
- (f) work in a way that distracts or harasses any other authorised user or member of the public;
- (g) remove, deface or corrupt notices placed by a CSU employee regarding the use of CSU computing or communication facilities;
- (h) use the CSU computing system to support the operation of a non-CSU related business, enterprise or activity;
- (i) use the CSU computing system to store, transfer or reproduce copyrighted material.

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:
- (a) counselling;
 - (b) removal or restriction of access to services;
 - (c) formal censure;
 - (d) reimbursement of expenses incurred;
 - (e) withholding of a salary step or point;
 - (f) demotion by one or more salary steps or points;
 - (g) demotion by one or more classification levels; or
 - (h) termination of employment.

21. STUDENTS

- 21.1 Where the Executive Director, Information Technology (or nominee) is of the opinion that a student has breached the provisions of this policy or that the breach may amount to misconduct, the Executive Director, Information Technology (or nominee) may suspend the student's access to CSU computing and communication facilities for a period of up to two (2) weeks pending investigation under the provisions of the *Student General Misconduct Rule*.
- 21.2 The Executive Director, Information Technology (or nominee) may exercise the authority granted under clause 22.1 more than once.

22. ALL AUTHORISED USERS OTHER THAN EMPLOYEES OR STUDENTS

Any authorised user, other than an employee or student of CSU, who is found by the Vice-Chancellor (or nominee) to have breached the provisions of this policy may be subject to:

- (a) termination, restriction or suspension of their access to CSU computer or communication facilities;
- (b) reimbursement of expenses incurred; and/or
- (c) any other such action that the Vice-Chancellor may deem appropriate.

23. REPORTING OF BREACH

CSU may report any breach of this policy that may require investigation to the police or any other appropriate authority external to CSU.

Table of amendments

Version number	Date	Short description of amendment
V2.0	17/10/2001	
V2.1	18/11/2005	Re-formatted.
V2.2	18/08/06	Amend cl.10, 22.1 Delete cl.22.2 Insert new cl.22.2
V2.3	27/10/08	Amend 4.3a,b,c,d,g, 72, 9.2, 9.3c,10, 13.1, 13.2(b,e,f),13.4, 14.1, 14.1(b), 14,2,18.2, 20,2, 23(a) Delete 3(d), 17.3 Insert 21.2(b) 18.3, 18.4, 17.4(h), 4.2(h), 13.4, 3(b,d,l,j)
V2.4	3/12/08	Insert 21.2(d), 13.5 Amend 13.1, 19.3
V3.0	20/07/09	Sect 18 Moved to Section (12) moved to Part 1 and renumber document Insert 5.3(h), 12.5, 13.2, 19.4(h) Remove sec 14.1, sec 20, 13.2, 18.2, 19.3 Edit 4.1(d), 4.3(a), 8.3,15.3(f), 18.2(f,i), Sec 23