Computing and Communications Facilities Use Policy

Section 1 - Purpose

(1) Charles Sturt University (the University) provides an extensive range of computing and communication facilities for use by staff, students and other authorised users.

(2) The conditions and obligations associated with authorised use of the University's computing and communication facilities are set out in this Policy.

(3) The objectives of this Policy are to:

a. facilitate the efficient, effective, responsible and lawful use of the University's computing and communication facilities;
b. safeguard the interests of the University and all authorised users of its computing and communication facilities; and
c. provide guidelines and instructions to authorised users in the appropriate use of the University's computing and communication facilities.

Scope

(4) This Policy applies to all authorised users of the University'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 the University or elsewhere.

References

(5) This Policy shall operate in conjunction with:

a. the 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 CSUNet Access Policy, that sets out the University's corporate responsibilities and obligations in regards to its communications and network infrastructure;
d. CSU Records Management Policy;
e. the Information Technology Equipment Purchasing Policy, that sets out the procedures for the purchase and charging of mobile telephones used for official purposes by employees of the University;
f. the Code of Conduct, that aims to foster and maintain public trust and confidence in the integrity and professionalism of the staff of the University;
g. the Student Misconduct Rule 2020;
h. the Spam Act 2003; and
i. the Telecommunications Act 1997.

Section 2 - Glossary

(6) For the purpose of this Policy:

a. Authorised user - means and refers to:
    i. an employee of the University;
    ii. a student of the University;
    iii. a person who holds an honorary or visiting appointment;
    iv. any external organisation or person that has a commercial arrangement with the University;
    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 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, Division of Information Technology (or nominee) as an authorised user, e.g. a member of the University Council.

b. Communication facilities - include, but are not restricted to, the following items:
    i. email;
    ii. facsimiles;
    iii. Internet;
    iv. pagers;
    v. satellite communications equipment;
    vi. telephones: landline and mobile;
    vii. two-way radios;
    viii. forums, blogs, wikis podcasts, vodcasts and other internet based communications tools.

c. Computing facilities - include, but are not restricted to, the following items:
    i. computer hardware, desktop and laptop computers, computer terminals, er mobile phones and other portable computing devices
    ii. peripherals such as printers, scanners, digital cameras
    iii. media, CD-ROMs, DVDs, Blu-Rays, disks and memory storage devices;
    iv. computer software and firmware;
    v. network connections (both wired and wireless);
    vi. operating and user manuals;
    vii. video conferencing and other presence technologies.

d. Employee - means and refers to any staff member of the University, including a person employed by the University on a casual basis.

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

ii. 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;
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 orientation and gender identity;
v. defames or could be reasonably anticipated to defame, any person, institution or company.

f. Student - means and refers 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 comprising subjects drawn from a course or courses leading to an award or awards of the University.

Section 3 - Policy

Part A - Network Security

(7) 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.

(8) 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.

(9) In particular, the Executive Director, Division of 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 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;
b. deal with existing or potential threats to the security and integrity of the University's computing and communication network;
c. prevent unauthorised access to and usage of the University's computing and communication network and facilities;
d. restrict the use of any University computer or communication facility that impedes the secure or efficient operation of the University's network;
e. 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;
f. remove or disable access to unauthorised equipment from the University's network;
g. 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; and
h. remove or delete without notice any data, material or software that is in breach of copyright legislation.

Part B - Disclaimer

(10) The University shall make available a range of computing and communication facilities to employees, students and other authorised users. 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.

(11) 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.

(12) 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 C - Provisions For Use By All Authorised Users

Prohibited Use of Computer and Communication Devices

(13) The use of any University computer or communications facility to make, send or store fraudulent, unlawful, harassing or abusive calls or messages is prohibited.

(14) The use of any University 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).

(15) 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 6e of this Policy.

(16) The prohibitions contained within clause 15 shall not apply where an authorised user is engaged in a responsible and honest search for a valid academic or research purpose.

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

(18) 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, Division of Information Technology (or nominee) in the first instance.

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

Login Identification

(20) 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.

(21) The provisions of clause 20(a-e) shall not apply:

a. 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
b. 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).

(22) 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, Division of Information Technology (or nominee).

Security

(23) 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.

(24) 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 the University's computing and communication facilities.

(25) An authorised user shall not, without the written authorisation of the Executive Director, Division of Information Technology:

a. examine, copy, rename, change or delete programs, files, data, messages or information belonging to the University or any other authorised user;
b. use the University's computing or communication facilities for profit-making or commercial activities;
c. modify any hardware or software;
d. 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.

(26) The provisions of clause 25(a-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.

Spam and Bulk E-mail Messages

(27) Distribution of bulk (spam) e-mail messages (all system users' e-mail) on the University'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.

Copyright

(28) 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.

(29) An authorised user should consult the University's copyright web page for further information concerning copyright restrictions and obligations or contact their campus library.

Confidentiality

(30) 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.

(31) The University reserves the right to monitor and audit the use by authorised users of the University computing and communication network and facilities and conduct an investigation where it has reasonable grounds that a breach of this Policy has occurred.

(32) 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.

(33) Investigations are conducted after receiving the permission of the Executive Director, Division of Information Technology (or nominee), and take into account privacy implications and with direction to the underlying reason for the investigative audit.

(34) 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; and
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 D - Obligations of Employees

Obligations

(35) In addition to the conditions and privileges of use set out in Parts A, B and C of this Policy, all employees shall ensure that:

a. the use of University computing and communication facilities is directed toward achievement of the academic and administrative goals of the University;
b. the University computing and communication facilities are used in a manner which is lawful, efficient, proper and ethical;
c. the University 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.

(36) 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 University computing or communication facility;
c. abuse, remove or tamper with any of the computing or communication facilities provided by the University;
d. work in a way that distracts, defames or harasses any other authorised user or member of the public;
e. use the University computing system to support the operation of a non-University related business, enterprise or activity;
f. use the University computing system to store, transfer or reproduce copyrighted material.

Private Use of Charles Sturt University (the University) Computing and Communications Facilities

(37) 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. Consequently, the University will allow, as a privilege, reasonable use of University 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 the University information technology facilities.

(38) An employee shall not use University 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;
c. downloading or uploading files with prohibited, inappropriate or illegal content including that which infringes copyright;
d. excessively accessing online content via the Internet such as computer games, video and audio content streaming, online messaging and chat;
e. accessing or transmitting prohibited data or material.

(39) The prohibitions contained in clause 38 c, d and e shall not apply where an employee is required to carry out such activities in the performance of his or her official duties.

(40) 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.

(41) 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.

Mobile Phones Used for Official Purposes

(42) 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:
    i. monitor University equipment and services outside normal working hours;
    ii. attend to an emergency or breakdown on the premises of the University;
    iii. 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 the University); or
    iv. 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.

(43) The University Mobile Phone Use 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 the University's Mobile Phone Use 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.

Confidentiality and Privacy

(44) 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.

(45) 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).

(46) 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.

(47) 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).

Record Keeping

(48) All electronic business communications are official University records and subject to the same standards of record keeping that apply to "paper" records.

(49) 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.

(50) An employee shall not breach obligations that relate to applicable standards of record keeping.

Part E - Obligations of Students

(51) In addition to the conditions of use set out in Parts A, B and C of this Policy, all students shall be accountable for the particular obligations as set out in Part E of this Policy.

(52) 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 University computing or communication facility;
c. abuse, remove or tamper with any of the computing or communication facilities provided by the University;
d. store data in an area unauthorised for such storage;
e. collect or discard the output of any other authorised user from the University'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 University employee regarding the use of University computing or communication facilities;
h. use the University computing system to support the operation of a non-University related business, enterprise or activity;
i. use the University computing system to store, transfer or reproduce copyrighted material.

Part F - Obligations of Authorised Users Other Than Employees and Students

(53) In addition to the conditions of use set out in Parts A, B and C of this Policy, all 'other' authorised users other than employees and students shall be accountable for the particular obligations as set out in Part F of this Policy.

(54) Subject to the provisions of clause 55, 'other' authorised users shall only use University 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.

(55) 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 University computing or communication facility;
c. abuse, remove or tamper with any of the computing or communication facilities provided by the University;
d. store data in an area unauthorised for such storage;
e. collect or discard the output of any other authorised user from the University 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 University employee regarding the use of University computing or communication facilities;
h. use the University computing system to support the operation of a non-University related business, enterprise or activity;
i. use the University computing system to store, transfer or reproduce copyrighted material.

Part G - Breach of Policy

Employees

(56) 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.

(57) 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.

Students

(58) Where the Executive Director, Division of 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, 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 pending investigation under the provisions of the Student Misconduct Rule 2020.

(59) The Executive Director, Division of Information Technology (or nominee) may exercise the authority granted under clause 58 more than once.

All Authorised Users Other Than Employees or Students

(60) Any authorised user, other than an employee or student of the University, 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 University computer or communication facilities;
b. reimbursement of expenses incurred; and/or
c. any other such action that the Vice-Chancellor may deem appropriate.

Reporting of Breach

(61) The University may report any breach of this Policy that may require investigation to the police or any other appropriate authority external to the University.

Section 4 - Procedures

(62) Nil.

Section 5 - Guidelines

(63) Nil.

Status and Details

Status	Historic
Effective Date	22nd May 2014
Review Date	30th June 2018
Approval Authority	Deputy Vice-Chancellor (Administration)
Approval Date	7th May 2014
Expiry Date	31st July 2022
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Timothy Mannes
Enquiries Contact	Division of Information Technology