Information Technology Conditions of Use Policy

Section 1 - Purpose and Scope

(1) The purpose of this Policy is to specify the conditions of use in relation to Technology Resources.

(2) This Policy applies to all Users of Technology Resources.

Section 2 - Definitions

(3) For the purposes of this Policy, the following definitions apply:

a. Digital Communications means any form of electronic communication managed by the University including voice, video, email, instant messaging, social media, conference calls (voice and video), chat, file transfer and application and data sharing.
b. Technology Resource means any hardware, software, device, network or other technology provided by the University for the purposes of teaching, learning, administration or other University-related business. This includes all forms of digital communications.
c. User means any staff member, student, or visitor to the University that uses any form of University Technology Resource.
d. Unauthorised Software means any software that has not been reviewed by Technology Services prior to installation on a University device. This includes, but is not limited to, games and peer-to-peer file sharing programs.

Section 3 - Policy Statement

(4) The University provides Technology Resources to support teaching, learning, research and administration based activities. The use of, and access to, Technology Resources is subject to relevant state and federal laws and all relevant University Policies, Procedures and Codes of Conduct.

(5) All Users are responsible for using Technology Resources in accordance with their intended and authorised purposes.

(6) All Users must exercise responsible, lawful, ethical and appropriate behaviour when accessing Technology Resources. Inappropriate use of these services may be deemed misconduct and dealt with accordingly, including loss of access to services.

(7) The Chief Information Officer is responsible for ensuring this Policy is up to date and enforced.

(8) In conjunction with Technology Services, Heads of Work Units are responsible for providing education and awareness to ensure their staff and students comply with this Policy.

Section 4 - Conditions of Use

General Use

(9) Users are responsible for:

a. respecting the privacy of others at all times;
b. reporting all faults and suspected faults to the Service Desk as soon as practicable;
c. ensuring they comply with the Social Media Policy and Social Media Procedures.

(10) Users are not permitted to do the following:

a. add an individual to an email distribution group without their consent, except where it pertains to official University business;
b. circumvent security systems or controls, exploit system vulnerabilities, or use any technology designed to locate such vulnerabilities except where authorised by the Chief Information Officer;
c. delete or alter data except as required by their authorised University activities;
d. install or intentionally download Unauthorised Software on University computers;
e. use or share software for purposes outside the specific terms and conditions or license agreement;
f. intentionally download or make available videos, music or pictures that breach the Copyright Policy or any copyright legislation;
g. interfere with or connect non-University networking or telecommunications equipment (eg. server hardware or peripherals, telecommunication services or devices, or data cabling) to the University network, except where authorised by the Chief Information Officer.
h. repair or interfere with, including by adding any devices such as hardware or components, telecommunication services, or data cabling, to any University Technology Resources except where authorised by the Chief Information Officer;
i. use another person's login or password, share your login or password with any other person or entity, attempt to gain unauthorised access to any computer service, or use a false identity to gain access to Technology Resources;
j. use University email distribution groups for anything other than University business.
k. use Technology Resources:
    i. for advertising, sponsorship, profit making, commercial activities except where it is clearly related to University purposes and authorised by the Head of Work Unit;
    ii. for gambling;
    iii. in ways which are likely to corrupt, damage or destroy data, software or hardware, whether inside or outside the network, and whether belonging to the University or not;
    iv. to access, store or transmit pornographic material or sexually explicit material, images, text or other offensive material unless authorised to do so by the Head of Work Unit and only where such data is in connection with teaching or research;
    v. to cause embarrassment or loss of reputation to the University;
    vi. to collect, use or disclose personal information in ways that breach relevant state or federal legislation, or the University's Privacy Management Plan;
    vii. to harass, abuse, discriminate, or vilify any other person within or beyond the University; and
    viii. to intentionally create, transmit, distribute or store any offensive information, data or material that breaches any State or Commonwealth law.

(11) The University reserves the right to audit and remove any illegal material from University Technology Resources without notice.

Internet Usage

(12) Internet usage must comply with this policy and other relevant University policies and procedures.

(13) Internet access is provided to all staff and students for the primary purpose of study, research and fulfillment of work-related functions. Internet may be used for incidental personal use, subject to compliance with this Policy.

(14) Internet usage levels will be periodically checked, and any users found to have excessively high usage not associated with intended or authorised use may be investigated and disciplinary action may be taken.

Privacy and Data Collection

(15) Access controls will be used to limit User access to systems or information to ensure that the confidentiality, integrity and availability of Technology Resources are maintained.

(16) The University creates and monitors logs of all activity undertaken on Technology Resources. This monitoring may reveal information such as which Internet servers have been accessed by employees, and the email addresses of those with whom they have communicated. This information will be managed in accordance with the University's Privacy Management Plan.

(17) Digital Communications are records of the University and may be accessible under the Government Information (Public Access) Act 2009 or relevant privacy legislation. The University may also be required to retain Digital Communications for a set period of time in accordance with the State Records Act 1998.

Cybersecurity

(18) Information and data transmitted over the internet or via email is capable of being intercepted, traced or recorded by others. The University cannot guarantee the confidentiality of any information stored on any University computer or transmitted through its network. Users should exercise caution with confidential information.

(19) All Users must take reasonable steps in relation to cybersecurity, including:

a. ensuring passwords are kept confidential and not disclosed or shared;
b. ensuring passwords are strong, for example using at least eight characters, the use of at least one upper case alpha, one numeric and one special character;
c. updating passwords when they expire periodically;
d. enabling passcodes on mobile devices;
e. exercising caution regarding phishing and malware by avoiding opening attachments or clicking on web links in emails unless the source and destination link is known and trusted ;
f. ensuring anti-virus software is installed;
g. ensuring the most recent version and updates have been installed;
h. ensuring data is stored appropriately (cloud drives);
i. Backing up data regularly and before traveling; and
j. Refraining from using free or gifted USB or similar devices unless from a trusted source.

(20) The University will never ask Users to reveal or confirm their passwords.

(21) If a User becomes aware of, or suspects that a security breach has occurred, they must immediately report the incident to the Service Desk.

(22) The University will report data breaches as required by law, or where deemed appropriate by the Chief Information Officer in consultation with the University Legal Office.

(23) When traveling, Users must take additional steps to protect Technology Resources and information stored on them. Users should:

a. only take Technology Resources that are required when traveling;
b. refrain from engaging in sensitive or confidential work on public computers, non-trusted networks and free or public Wi-Fi; and
c. be mindful of politically sensitive or potentially illegal information depending on destination.

Phishing and Spam

(24) Phishing emails are designed to lure in unsuspecting victims and these emails can steal your identity, infect your computer and result in ransomware. Ransomware encrypts all of the files on your computer including any files on connected drives you have access to. These files cannot be unencrypted and so rely on the integrity of restoring from backups.

(25) Users must apply the following general principles to avoid damage to Technology Resources:

a. never click a link in an email or open an attachment unless it is from a trusted source.
b. be aware that Technology Services will not send an email request to confirm an account or password details.
c. contact the service desk to report suspect emails.

(26) The University will take steps to reduce the prevalence of unwanted or unsolicited email (spam), including by applying automatic filters and rules.

Technology Purchasing

(27) All procurement of Technology Resources (including software hosted on site or in the cloud, software as a service, software subscriptions and hardware) must be reviewed by the Chief Information Officer prior to being purchased. In consultation with the relevant work unit, the Chief Information Officer will consider data, security, contractual, financial, solution viability and legal implications of the intended purchase and consumption.

(28) Any purchase of Technology Resources must be made and comply with the University's Procurement Policy and Procurement Procedures.

(29) Technology Services will not provide any support for Technology Resources that were not reviewed and approved by the Chief Information Officer prior to procurement.

(30) The physical security of computer equipment is the responsibility of the relevant Work Unit. Each Work Unit should take adequate steps to ensure equipment is secure from loss or theft.

(31) Technology Services will maintain a Software Asset Register of all software purchased by Technology Services.

(32) The purchasing Work Unit must retain the license agreement for audit and compliance purposes.

(33) Technology Services will audit Technology Resources and where required, remove any Unauthorised Software.

(34) Technology Services provides support for all software listed as part of the University's Standard Operating Environment.

Section 5 - Digital Communications

Email

Student Email Accounts

(35) The University will provide all enrolled students with a University email account for the period of their enrolment.

(36) The University will use a student's University email account as the primary form of communication with students.

(37) Students are responsible for regularly accessing and reviewing University email.

Staff Email Accounts

(38) The University will provide all staff with a University email account for the period of their employment.

Non-Standard Email Accounts

(39) The University may also provide a University email account to:

a. members of the University Council;
b. adjunct and emeritus staff;
c. trainee staff;
d. contractors; and
e. industry partners.

(40) Staff may request a Non-Standard Email Account by sending a request to the Service Desk. The request must be authorised by the relevant Head of Work Unit or Executive member.

Generic Accounts and Aliases

(41) Staff may request the creation of a generic email address (e.g. policies@scu.edu.au) where it is necessary for business process and workflow purposes. Staff must submit a request for a Non-Standard Account to the Service Desk. The request must be authorised by the relevant Head of Work Unit or Executive member.

Bulk Email Groups

(42) The University utilises a number of bulk email groups for the broadcast and dissemination of information to staff and students.

(43) Technology Services automatically subscribes staff and student email accounts to the relevant bulk email groups.

(44) Technology Services, or another nominated Work Unit, will moderate messages sent to bulk email groups.

Staff and Student Email Discussion Forums

(45) The University provides email discussion forums for matters that fall outside the purposes of the University's bulk email groups. Discussion forums may only be used by current staff or students of the University.

(46) All University Rules, Policies and Procedures and Codes of Conduct, apply to the use of, and participation in, University email discussion forums.

(47) Language or content that is considered to be threatening, defamatory, abusive or discriminatory is in breach of the University's Code of Conduct, and is not permitted on University discussion forums and will be dealt with

accordingly. Harassment and bullying will not be tolerated.

(48) Commercial advertising is not permitted on any University discussion forum.

(49) Users should report any offensive materials they find through the University Complaints Management Framework.

Representation

(50) Users must be aware that Digital Communications using a University email account may be construed to be representative of the University's position. Where Users do not have the authority or are not aware of the University's position or where their personal views may vary from that of the University, such correspondence must clearly state that the opinion expressed is that of the writer, and not necessarily that of the University.

(51) Where a staff member is representing the views of the University, then a notation must be included in the email identifying the individual and the position held within the University.

Access to Emails

(52) Within their relevant Work Unit, Heads of Work Units may request access to data and information stored on University computers or databases by sending a request to the Service Desk, subject to approval from Chief Information Officer.

(53) The University will not grant access to a University email to any person other than the original sender or intended recipient, except where:

a. Access is required for a staff member to undertake their duties;
b. as required by law;
c. where there is substantial reason to believe that breaches of the University's policies have taken place; or
d. by an authorised delegate for the purpose of dealing with an application under the Government Information (Public Access) Act 2009.

(54) University system administrators will, as part of their role, have full access to the University email and other network systems. System administrators will only access email and network systems in accordance with their employment duties and applicable legislation.

(55) The University will retain archived or backup copies of all Digital Communications.

(56) Heads of Work Unit may request out of office or other notifications be put in place on behalf of absent or unavailable staff.

Section 6 - Breaches of this Policy

(57) Users must report breaches or suspected breaches of this Policy to their supervisor, lecturer, teacher or Head of Work Unit as soon as possible.

Staff

(58) A breach of this Policy by a Staff member may be treated as misconduct depending on the nature of the breach. Breaches shall be dealt with as provided for under the relevant section of the University's Enterprise Agreement, or in accordance with University Policies and Procedures.

Students

(59) At the discretion of the University any breach of this Policy may be treated as non-academic misconduct which will be dealt with under the Rules - Student Academic and Non-Academic Misconduct Rule.

Section 7 - Service Desk

(60) Users may request advice, support and general assistance regarding this policy via the Service Desk by:

a. emailing servicedesk@scu.edu.au; or
b. phoning (02) 6620 3698 during business hours; or
c. visiting the online Service Desk.

(61) The Service Desk can provide limited support in relation to basic configuration and advice in relation to personal devices. The University takes no responsibility and will not be held liable for any actual or perceived damage, misconfiguration or hardware issues regarding personal equipment arising from advice provided by the Service Desk.

Status and Details

Status	Current
Effective Date	18th February 2019
Review Date	1st December 2026
Approval Authority	Vice Chancellor
Approval Date	18th February 2019
Expiry Date	Not Applicable
Responsible Executive	Jack Williamson Vice President (Strategy & Technology)
Head of Work Unit	Jack Williamson Vice President (Strategy & Technology)
Enquiries Contact	Darron Richardson Director, Cyber Security --- Vice President (Strategy & Technology) Portfolio