Acceptable Use of ICT Resources - Procedures

1. Purpose of procedures

1.1 These procedures provide clients with additional protocols to be followed, to be read in conjunction with the Acceptable Use of ICT Resources – Governing Policy.

2. Definitions

Please refer to the University's Glossary of Terms for policies and procedures. Terms and definitions identified below are specific to these procedures and are critical to its effectiveness:

Clients includes Staff, Student or Affiliates who, based on their relationship with the University, need access granted to University ICT resources.

Staff are defined as individuals who hold an active employment contract with the university and are present in the University's Human Resources and Payroll System.

Student is defined as an individual who is currently enrolled in a program at the University. However, where explicitly stated, student may include an applicant to the University, a student on a leave of absence, or a former student (alumni) who has completed their program and are present in the University's Student Information System.

SPAM is defined in the SPAM Act 2003 as unsolicited commercial electronic messages.

Affiliate is defined as an individual who has a bona fide relationship with the University for which approval has been gained to offer access to various ICT resources. This may include adjunct or visiting appointees, volunteers, contractors and consultants.

ICT Resources includes a range of information and communication technology hardware, software and services that may be owned, contracted, licensed, managed or otherwise facilitated by the University for use by the University and its authorised clients.

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Director, Information Technology

FIRST APPROVED

5 December 2019

LAST AMENDED

10 December 2019

REVIEW DATE

5 December 2024

STATUS

Active

3. Protocols for electronic communications

3.1 Information management

3.1.1 Staff and affiliates are reminded that all University electronic messages, inbound and outbound, business and personal, are the property of the University.

3.1.2 Staff are advised all University electronic messages that provide evidence of University business actions, activities and decisions are considered records of the University and must be captured in an approved records management system, in accordance with the Information and Records Management – Procedures.

3.1.3 All University electronic messages, regardless of storage location, may be subject to applications under the *Right to Information Act 2009* (Qld), and may be subpoenaed as evidence in a court of law.

3.2 Unsolicited material

3.2.1 The University reserves the right to employ network protection software and/or hardware, including virus protection systems, firewalls and automated scanning of incoming emails prior to delivery to recipients. Suspect emails may be blocked or deleted by these systems. Some emails may be quarantined, if safe or reasonably safe to do so, pending a decision by the intended recipient to choose whether the email is released or deleted.

3.2.2 Other than as reasonably required to perform network protection duties, the University is restricted by law from making copies of quarantined emails or forwarding them to persons other than the intended recipient, prior to the emails becoming accessible by the

intended recipient. Network protection duties, including any manual scanning of emails will be undertaken in accordance with Queensland Government's Information Standard IS18 and the ISO/IEC 27001 standard.

3.2.3 Staff or affiliates receiving inappropriate material from the internet or through an email should delete such material from the University systems immediately and notify their supervisor/manager of their actions. Such an action should not constitute misuse.

However, for all clients, copying or forwarding of inappropriate or unacceptable material by whatever means constitutes unauthorised use.

3.2.4 Unsolicited emails, that are not related to University business actions, activities or decisions, are classified as transitory records and can be deleted without disposal approval.

3.3 Broadcast communications

3.3.1 Electronic messages may only be broadcast to clients under circumstances where it is a normal part of work practice (e.g. a lecturer emails their students) or where authorisation from the Cost Centre Manager has been received. In general, communications to all staff should be managed through the staff intranet (MyUniSC).

3.3.2 All broadcast emails to larger student groups (beyond students enrolled in a course) are managed through Student Communications, in Student Services and Engagement.

3.3.3 Any outgoing electronic broadcast message that is commercial in nature must conform to the *SPAM Act 2003* (Cth) and be authorised by the Cost Centre manager. Where the electronic message is directed to individuals who are not clients (e.g. external individuals) the message is to be authorised by the Director, Marketing.

3.3.4 Use of social media for broadcast communication is detailed further in the Social Media – Managerial Policy.

4.4 Staff mailboxes

4.4.1 Each client is responsible for their own electronic email account and the use of that account. Generic email accounts (e.g. careers@usc.edu.au) will have an assigned individual responsible for the account. Cost Centre managers are responsible for the approval of generic email accounts and email accounts granted to external organisations and individuals for which they are responsible.

4.4.2 Clients should formally identify themselves and their position within the University, particularly for all business emails that are sent external to the University.

4.4.3 Staff on leave should provide an out-of-office automated response, directing queries to another staff member. If approved by the Cost Centre manager, a staff member may use the appropriate software functionality to delegate access to another staff member to view and/or manage their mailbox, however under no circumstances should a staff member share their password. If a staff member on leave is uncontactable, and where it is necessary for business purposes, the relevant Cost Centre manager may authorise an appropriate member of IT staff to gain access to a mailbox.

5. Protocols for software

5.1 University clients who acquire and/or install software must obtain permission from IT prior to downloading and are responsible for ensuring that they do so in accord with the relevant IT Services procedures. In all instances clients must ensure that software is used in accordance with the licence terms and conditions as set out by the copyright holder.

5.2 Software sourcing and acquisition is conducted through Information Technology in consultation with appropriate staff to ensure suitable licence terms and conditions, pricing and compatibility with the University's MOE. Copies of software and documentation may be created for backup and disaster recovery purposes as permitted by the licence terms and conditions.

5.3 Where software is subject to a periodic renewal, this renewal may be subject to review of continuing business needs. Where a renewal is required to retain a valid software licence, but the licence is not subsequently renewed, the software will be withdrawn from access.

5.4 The disposal of software media, backup and documentation should be managed in accordance with the software licence terms and the Information and Records Management – Procedures. In all cases approval must be sought from Information Management Services prior to the commencement of any disposal activities.

5.5 Where possible, controls will be in place within the University to prevent the making or use of illegal software copies, or installation of unauthorised software onto University ICT resources. These controls will include effective measures to verify compliance with acquired software licences and University standards.

5.6 The University reserves the right to remove unauthorised or illegal software, and to do so without prior notification where the risk to the University is considered to be significant.

5.7 Internal software audits will be conducted periodically on University computers. External audits, when requested by vendors, their agents or other auditing bodies, are to be directed to the Director, Information Technology in the initial instance.

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Governing Policy

- Adopting Cloud-based Services - Procedures
- Anti-Discrimination and Freedom from Bullying and Harassment - Governing Policy
- Copyright - Governing Policy
- Copyright - Procedures
- ICT Security - Operational Policy
- Information System Operations - Procedures
- Intellectual Property - Governing Policy
- Intellectual Property: Commercialisation - Procedures
- Intellectual Property: Commercialisation Revenue - Procedures
- Intellectual Property: Student IP - Procedures
- Intellectual Property: Transfer of Rights to Creators - Procedures
- Social Media - Operational Policy
- Social Media - Procedures
- Student Conduct - Governing Policy

LINKED DOCUMENTS

- Acceptable Use of ICT Resources - Governing Policy

SUPERSEDED DOCUMENTS

- Software - Governing Policy
- Telephone - Managerial Policy
- Electronic Mail - Managerial Policy

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2002 (Qld)
- Public Sector Ethics Act 1994 (Qld)
- Queensland Information Standards
- Copyright Act 1968 (Cth)
- Privacy Act 1988 (Cth)
- SPAM Act 2003
- Information Privacy Act 2009 (Qld)
- Student Charter