

Acceptable use of Information Technology (IT) facilities

POLICY NO: C - 22.1

Date of Authorisation:

Effective Date:

Date of Last Amendment:

Superseded documents: Use of University Information Technology (IT) Facilities

Reference Authority: Pro Vice Chancellor Strategy and Planning;

Director, Information Strategy and Technology Services

Related documents: This Policy must be read in conjunction with the documents listed in Appendix A. Those documents address specific implementation issues such as internet use, email and privileged access to systems.

Contact Person: Any person who requires assistance in understanding any aspect of this document should contact Director Information Strategy and Technology Services (ISTS)

1. Overview

The University provides Information Technology facilities (IT facilities) to support its teaching and learning, research, administrative and business activities. IT facilities includes all computing and communication equipment, software, services, data and dedicated building space used in connection with information technology, which is owned by, leased by or used under licence or agreement by the University. The University recognises its responsibility to ensure the appropriate use of its IT facilities and that it must be protected from damage or liability resulting from the unlawful or inappropriate use of its IT facilities.

2. Scope

This Policy applies to users with authorised accounts (as defined below) to access the University's IT facilities.

3. Users with Authorised Accounts

3.1 It is a requirement that every person who accesses University IT facilities must have an authorised user account for their exclusive use.

3.2 Authorised accounts will only be issued to staff employed by the University, currently enrolled students, visiting academics, contractors or consultants engaged by the University, or other recognised affiliates of the University. In addition, access to particular systems and types of use may require authorisation by the relevant Unit Director/Manager, Research Institute Director, Head of School or equivalent.

3.3 All users with an authorised account must comply with this policy when using the University's IT facilities.

4. Other Users

4.1 This policy recognises that some University IT facilities are provided for the use of members of the general public who do not have any formal relationship with the University. Examples of such facilities are University web sites that are not subject to some form of access control, and limited access to the electronic information resources accessible from the Library where this is permitted by license.

4.2 These users will not be issued with user accounts, and will only be subject to sections 5.3 and 5.4 of this policy. In addition, their use of University IT facilities must comply with State and Commonwealth laws and any additional Guidelines issued by the University in relation to their use of the facilities.

5. Acceptable Use

5.1 IT facilities are provided to support the University's teaching and learning, research, administrative and business activities.

5.2 IT facilities are not provided for recreational or personal use unless specifically stated otherwise in the guidelines listed in Appendix A.

5.3 Users of University IT facilities must comply with the University's requirements for acceptable use. Specific activities that constitute unacceptable use include but are not limited to:

5.3.1 deliberate, unauthorised corruption or destruction of IT facilities (including deliberate introduction or propagation of computer viruses.

- 5.3.2 deliberate, unauthorised access to IT facilities
- 5.3.3 unauthorised use of data or information obtained from the use of IT facilities
- 5.3.4 use of IT facilities to access, create, transmit or solicit material which is obscene, defamatory, discriminatory in nature, or likely to cause distress to some individuals or cultures, where such material is not a legitimate part of teaching and learning or research (if the material is a legitimate part of teaching and learning or research, an appropriate warning should be given)
- 5.3.5 transmission or use of material which infringes copyright held by another person or the University
- 5.3.6 violation of software licensing agreements
- 5.3.7 use of IT facilities to transmit unsolicited commercial or advertising material
- 5.3.8 deliberate impersonation of another individual by the use of their login credentials, e-mail address or other means
- 5.3.9 violation of the privacy of personal information relating to other individuals
- 5.3.10 unauthorised disclosure of confidential information
- 5.3.11 use of IT facilities to harass or threaten other individuals
- 5.3.12 unauthorised attempts to identify or exploit weaknesses in IT facilities
- 5.3.13 unauthorised attempts to make University IT facilities unavailable
- 5.3.14 use of University IT facilities to gain unauthorised access to third party IT facilities
- 5.3.15 use of University IT facilities in unauthorised attempts to make third party IT facilities unavailable
- 5.3.16 use which deliberately and significantly degrades the performance of IT facilities for other users (including the downloading of MP3 files not related to teaching and learning and research).
- 5.4 Users must also comply with the University's other policies and procedures and other Guidelines as released by ISTS.
- 5.5 If any unacceptable use of University IT systems is detected, it must be reported to ISTS.
- 5.6 Behavior which breaches this policy may also breach Commonwealth and State law.

6. User Accounts and Passwords

- 6.1 All user accounts must have one person nominated as the person responsible for that account.
- 6.2 Users are responsible for all activity initiated from their accounts, unless it is established that the activity was done by another person who gained access to the user's account through no fault of the user.
- 6.3 Users must select passwords that cannot be easily guessed and they must not divulge passwords to others, including other staff and students.
- 6.4 Users must not attempt to determine another user's password.
- 6.5 If the security of a password is compromised, it must be changed immediately.
- 6.6 Users are not permitted to authorise others to login using their account.
- 6.7 Passwords should be changed regularly.
- 6.8 Users are prohibited from using another user's account.

7. University Responsibility

The University will take reasonable steps to protect its IT facilities from unauthorised and unacceptable use.

8. Monitoring Use

The University reserves the right to monitor any and all aspects of its IT facilities to determine if a user is acting unlawfully or violating this Policy, the associated documents listed in Appendix A, or any other University policy or rule. Such monitoring may include, but is not limited to, individual login sessions, the internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user. Procedures relating to monitoring use are listed in Appendix A.

9. Compliance

- 9.1** Users of University IT facilities are responsible for adhering to the provisions of this Policy.
- 9.2** The University may take remedial action and suspend user access with or without prior notice in response to suspected breaches of this policy.
- 9.3** Breaches by staff or students that constitute misconduct will be addressed by the relevant staff or student disciplinary procedures. See Appendix A.
- 9.4** Sanctions for failing to comply with this Policy or the associated documents listed in Appendix A, may include:
 - 9.4.1** immediate withdrawal of access to IT facilities, with or without prior notice
 - 9.4.2** action taken under the University's relevant performance management scheme and/or disciplinary procedures for staff or for students.
 - 9.4.3** criminal or other penalties imposed by State or Commonwealth legislation
 - 9.4.4** financial compensation sought by the University.

10. Exceptions

Requests for exceptions to this policy must be authorised by the Director ISTS. Such requests must be made in writing and will be evaluated based on the case presented to support it.

11. Implementation and review

- 11.1** All Unit Director/Managers, Research Institute Directors, Heads of School or equivalent will be responsible for the implementation of this Policy in their respective areas of responsibility.
- 11.2** The Director ISTS is responsible for regularly reviewing this Policy.
- 11.3** The Director ISTS has authority to issue from time to time the Guidelines referred to in the Appendix due to changes in the law or changes in the practices of the University.
- 11.4** The Director ISTS has authority to amend Appendix A and any Guidelines issued.
- 11.5** Both the Guidelines referred to in Appendix A and any additional Guidelines are afforded the status of the policy.

12. Communication

- 12.1** Student and Academic Services and the Human Resources Unit are responsible for ensuring that all students and all staff members have access to this Policy through the University website and myUniSA.
- 12.2** This Policy will be included in the information package provided to all new members of staff.

Appendix A

1. Associated Documents

For information on the application of this policy see:

Guidelines for Staff on Use of IT Facilities including Email and the Internet

Guidelines for Students on Use of IT Facilities including Email and the Internet.

See also University policies and resources for staff and for students listed on the ISTS website.

Other University legislation and policies that may be relevant to implementation of the Policy on Acceptable Use of IT are:

Policy and procedures for the resolution of student grievances

Statute 7: Maintenance of Order

Security on Campus (C-9.1)

Prevention of violence on campus (C-19.0)

Anti-racism Policy (C-21.2)

Equal Opportunity Policy (C-2.3)

Sexual Harassment Policy (C-12.3)

Public Statements by Members of the University Staff(C-5.0)

University Activities Policy (C-20.1)

Code of Ethical Conduct (C-8/99)

Inclusive Language Policy (C-1.4)

Discrimination and harassment grievance procedures (academic and general staff)

2. Relevant Legislation

While not an exhaustive list, the following legislation is of particular relevance to the use of University IT facilities:

The Commonwealth Copyright Act (1968)

The Commonwealth Crimes Act (1914)

The Commonwealth Criminal Code Act (1995)

The South Australian Criminal Law Consolidation Act (1935)

The Commonwealth Cybercrime Act (2001)

The South Australian Equal Opportunity Act (1984)

Racial Vilification Act 1996 (SA)

The South Australian Freedom of Information Act (1991)

The Commonwealth Spam Act (2003)

The South Australian State Records Act (1997)

The South Australian Summary Offences Act (1953)

3. Relevant terms

Disciplinary procedures

The disciplinary procedures as outlined in the applicable industrial instrument shall apply to staff.

The disciplinary procedures as outlined in the applicable statute or policy shall apply to students.

Industrial Instrument - refers to the applicable Enterprise Agreement, Award, Australian Workplace Agreement, contract of employment or legislation.