ICT Policy

Category Operational
Version 1
First ratified April 2009
Last ratified April 2009

---

1. **Purpose**
    1.1. This policy provides direction for the protection of the ICT assets and operations of the Otago University Students' Association (OUSA).
2. **Interpretation**
    2.1. In this policy, unless the context otherwise requires:
        2.1.1. User means anyone who operates or interfaces with OUSA's Information & Communications Technology (ICT). It includes OUSA staff, officers and students (whether permanent, temporary or part-time), contractors, sub-contractors, consultants, official visitors or any other member of OUSA.
        2.1.2. Network means the OUSA's computer network and includes all hardware (including portable computers), software, floppy disks, CD-ROMs, other storage media, modems, and other network resources.
        2.1.3. Email includes all electronic communications, including electronic mail, messaging services, electronic bulletin boards, "chat" services and text messaging.
        2.1.4. Computer shall mean every item and kind of computer equipment, computer software, network, CD-ROM, memory stick and related items and equipment provided by OUSA or used on the OUSA network.
        2.1.5. ICT Manager in relation to any OUSA computer, means the person authorised by the OUSA Chief Executive Officer to control all ICT activities of the OUSA.
        2.1.6. Authorisation, unless otherwise stated, shall means consent from the OUSA ICT Manager.
        2.1.7. ICT (Information and Communications Technology) means any device or application used to convert, store, protect, process, transmit, share and/or retrieve information encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning.
3. **Computer Regulations**
    3.1. No user shall without authority:
        3.1.1. Access, or attempt to gain access, to any computer or network;
        3.1.2. Obtain, copy, or in any way remove any information from a computer;
        3.1.3. In any way modify or interfere with, or erase, any information on any computer or network;
        3.1.4. Use any computer system or facility in such a way as to contravene any requirements for its use notified by the ICT Manager;
        3.1.5. Remove, disconnect, tamper with or otherwise interfere with any physical component(s) of a computer system;
        3.1.6. Subvert, or attempt to subvert, any user identification and/or authentication scheme on any system;
        3.1.7. Cause or attempt to cause any computer system to fail or deny service to any authorised user;
        3.1.8. Divulge a password or code enabling access to a computer unless permitted to do so by the ICT Manager;
        3.1.9. Use or attempt to use a computer so as to cause costs to be incurred by any person or organisation without authorisation;

3.1.10. Use computer facilities to send or disseminate offensive, abusive, threatening or unnecessarily repetitive messages;

3.1.11. Use any software which has been unlawfully obtained;

3.1.12. Use any computer in such a way as to deliberately interfere with the reasonable use by another person of a computer, or any other facility;

3.1.13. Use any computer while masquerading as another user; or;

3.1.14. Assist any person to do any of the above.

3.2. Any user who is permitted to use any computer shall take reasonable precautions to secure his or her passwords, accounts, software and data.

3.3. All viruses detected on any computer or disk, must be reported to the ICT Manager as soon as detected to prevent the virus from contaminating the equipment further.

4. Email

4.1. All users who have an official OUSA email address associated with their computer account should make sure that email to this address is checked regularly.

4.2. All users are responsible for all email originating from their account.

4.3. Users may not send an email that purports to represent OUSA or its views, without proper authority. If there is any risk of misunderstanding, a disclaimer must be inserted in the body of the email.

4.4. All users shall comply with the Unsolicited Electronic Messages Act 2007.

4.5. No user shall without authority use OUSA’s email systems to:

4.5.1. Create or distribute chain letters, "junk" or "spam" (mass, unsolicited) mail;

4.5.2. Send anonymous email;

4.5.3. Disrupt another person’s activities;

4.5.4. Harass another person or send unwanted offensive material;

4.5.5. Forge email messages to make them appear to originate from another person;

4.5.6. Read, delete, copy or modify email under the control of other users without authorisation;

4.5.7. Pursue commercial activities, including sending "for-profit" messages or advertisements, unless on behalf of OUSA and with the appropriate authorisation;

4.5.8. Introduce viruses;

4.5.9. Download unauthorised software without approval; and;

4.5.10. Intentionally engage in illegal activities.

5. Internet Fair Use

5.1. Users must not use the Internet for proscribed use. Proscribed use includes but is not limited to:

5.1.1.1. Visiting sites or receiving communications that contain material that is obscene, objectionable, or likely to be offensive;

5.1.1.2. Gambling;

5.1.1.3. Soliciting for personal gain or profit;

5.1.1.4. Making or posting indecent remarks and proposals;

5.1.1.5. Uploading or downloading commercial software in violation of its copyright;

5.1.1.6. Passing off personal views as representing those of OUSA;

5.1.1.7. Any activity that violates New Zealand law; or;

5.1.1.8. Extensive private usage. Use is deemed to be extensive when it either interferes with normal network activity, or costs OUSA an unacceptable amount of money

5.2. OUSA owned computer facilities are provided to support the primary functions of OUSA and its administration. Personal use is allowed on most OUSA systems but only when the system is not required for its primary functions and, for staff members, only when it does not impede the work for which they are employed.

6. Connection of Equipment to the OUSA Network

6.1. All new software or equipment being added to the OUSA computer system or network requires appropriate authorisation.

6.2. The ICT Manager may authorise disconnection of equipment from the network if it is a threat to the integrity of the network either as a result of not adhering to this policy, or because of its nature.

6.3. Computers connected to the OUSA computer network should have up-to-date virus protection software installed and active at all times; and should have all relevant system security patches installed.

6.4. Network traffic is private. "Packet sniffing" (using network monitoring tools to eavesdrop on ‘packets’ passing through a network), or other unauthorized and deliberate attempts to read network information that is not intended for your use is not permitted without the appropriate authorisation.

6.5. No network devices (including modems) are to be connected to any portion of the network without the appropriate authorisation.

7. Breaches of this Policy

7.1. Any person who, in the opinion of the ICT Manager, is engaged in a breach of this policy may be immediately excluded from that system and have all associated computer activities suspended. Failure by that person to comply with instructions necessary for exclusion shall in itself constitute a breach of this policy.

7.2. Any person who interferes with regulations in this policy will be held liable for damage claims made against OUSA in relation to that interference. Further the person will be liable for the costs of detection and repair of breaches to security, damage to hardware, or any other costs incurred by OUSA in dealing with the consequences of a contravention of this policy.