

ICT User Policy

Responsible Officer	Director, Technology & Infrastructure
Contact Officer	Director, Technology & Infrastructure
Authorisation	CEO
Effective Date	13 December 2010
Associated Documents	AFTRS Code of Conduct Rules, Policies and Procedures for Students Guidelines on Sending Commercial Email Email Etiquette Guidelines Online Security Policy AFTRS Fraud Control Policy

1 Policy Name

Information & Communications Technology (ICT) User Policy

2 Preamble

This Policy provides the framework for the use and the security of AFTRS' Information and Communications Technology (ICT) resources. AFTRS is an Australian government authority. As such, AFTRS' ICT resources and those who use them are subject to the legislative requirements of the Australian government.

AFTRS' ICT resources facilitate AFTRS' business systems and its communications. These resources are an essential part of the toolkit AFTRS provides staff and students to meet its core functions in providing advanced education and training to talented students, industry professionals and industry practitioners. AFTRS also encourages strong links with industry organisations, and makes available the use of its ICT resources as appropriate to these groups, as well as to contractors and visitors as required.

3 Policy Scope

This policy applies to all AFTRS' staff and students as well as all other authorised users including visiting staff, guests, contractors and other users of AFTRS' ICT resources, onsite or externally.

4 Definitions

The following definitions apply to this policy:

- **Information & Communications Technology (ICT):** ICT includes all network systems, phone (including mobile) systems, desktop and laptop computers, software, and internal and external connections to the Internet via the AFTRS infrastructure. It extends to all current, emerging and future technologies.
- **Authorised Users:** All AFTRS staff including casual staff; all AFTRS students including all students enrolled in award courses and all students enrolled in short courses; all visitors, guests and contractors to AFTRS.

5 Principles

The following principles express the intent of this policy:

1. AFTRS will provide ICT resources to its staff, students and visitors, on-site and externally, as appropriate and according to need.
2. AFTRS requires all Users of its ICT resources to abide by the AFTRS Code of Conduct and to use its ICT resources in a legal, ethical and responsible way.

3. AFTRS takes all precautions to secure its ICT resources and to protect the privacy of individuals and confidentiality of material as appropriate. However Users need to be aware that the normal course of securing the system includes but is not limited to actions such as backup, logging of activity and monitoring general usage.
4. AFTRS may disclose electronic communications, records and other transactions to the appropriate authorities if legally required to do so.
5. AFTRS may terminate access to its ICT resources by any User if the User is found to be in breach of this policy.

6 Policy Statement

AFTRS provides ICT resources to staff and students and other Authorised Users for the purposes of teaching and research, production and creative work, events and exhibition and to conduct all other business and communications. All Authorised Users will use AFTRS' ICT resources for these purposes and exercise their use in a legal, ethical and responsible manner and according to this policy.

7 Conditions of Use

- 7.1 Authorised Users are required to use their assigned User-ID to access AFTRS' ICT Resources. Users are not to access ICT resources anonymously or by false identity.
- 7.2 All User-IDs that have been inactive for at least 60 days will automatically have the associated privileges revoked. System privileges will be re-established only after the respective User obtains approval from Human Resources, Student Services or departmental heads who will forward their recommendation to the Head, ICT and Services or the Director, Technology and Infrastructure.
- 7.3 The primary User of a computer is considered to be a custodian of the equipment. Computer equipment must not be moved or relocated without the approval of the Head, ICT and Services. If the equipment has been damaged, lost, stolen, borrowed or is otherwise unavailable for normal activities, the custodian must promptly inform the Head, ICT and Services or the Director, Technology and Infrastructure.
- 7.4 Users must not use ICT Resources for private business activities, however incidental personal use of ICT resources is permissible so long as:
 - it only uses a trivial amount of resources;
 - it does not interfere with productivity;
 - it does not pre-empt any AFTRS business activities; and
 - it is not used to make political, religious or other similar statements to any external recipient or organisation including but not limited to governments, the press and charities.
- 7.5 Software may only be loaded onto an AFTRS computer system in consultation with the Technology & Infrastructure division. Only those Authorised Users granted Administration privileges, by application, may load software themselves.
- 7.6 Users must not use AFTRS' ICT Resources to solicit, collect, use, disclose, alter or store personal information in any way that breaches the Privacy Act 1988.
- 7.7 Users must not use AFTRS' ICT resources to access, transfer or store, or reproduce, copy, communicate publicly or otherwise use, any material without an appropriate license to do so or is likely to contravene the Copyright Act, 1968. Applicable material may include, but is not limited to, software, images, artistic work, live pictures, computer games, film, music and video.
- 7.8 Users are forbidden to use ICT Resources to access pornographic material of any sort other than for the purposes of education and research. Transmission is not permitted under any circumstance.
- 7.9 It is illegal to harass, menace, defame, libel, vilify or discriminate against any person within or external to AFTRS. AFTRS' ICT Resources must not be used in a harassing, discriminatory, abusive, rude, insulting, threatening, obscene or otherwise inappropriate or illegal manner.
- 7.10 Users must not use ICT Resources in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to the School or to anyone else, whether inside or outside the network. Users may only delete and alter data as required by their authorised School activities.
- 7.11 All files downloaded from non-AFTRS sources via the Internet or received via the AFTRS email system must be screened with virus detection software prior to being used.

- 7.12 Computer systems provided by AFTRS must not be altered or added to in any way without the prior approval of the Head, ICT and Services or the Director, Technology and Infrastructure.
- 7.13 Users must not acquire, possess, trade or use hardware or software tools that could be used to evaluate or compromise AFTRS' information systems and networks or allow unauthorised access to AFTRS systems and information. This includes, but is not limited to, bridging AFTRS networks to the Internet or other external network and exposing systems or data through servers or other tools.
- 7.14 Users must not copy software provided by AFTRS without written permission from the Director of Technology and Infrastructure.
- 7.15 AFTRS reserves the right to revoke the system privileges of any User at any time.
- 7.16 AFTRS reserves the right to remove any material it views as offensive or potentially illegal from its ICT systems.
- 7.17 AFTRS reserves the right to delete, summarise or edit any information stored on AFTRS ICT resources.

8 Security, Privacy & Confidentiality

- 8.1 AFTRS takes all reasonable steps to secure its ICT Resources and ensure all confidential and personal information stored in its ICT Resources are electronically safeguarded as required by the Privacy Act 1988 and in accordance with best practice. However it cannot guarantee the protection of such confidential and personal information.
- 8.2 All files, communications and other data transmitted and stored on AFTRS' ICT Resources are regarded as AFTRS' records, including any data resulting from permitted incidental personal use.
- 8.3 A User must use reasonable efforts to ensure that every electronic document created by the User and designated as 'Confidential' displays the Confidential marking on the first screen shown to the recipient. All hardcopy computer output generated by a User and designated as Confidential must be marked Confidential. All computer-readable storage media containing Confidential information must have a Confidential designation on its external label. When not in use, this media must be stored in a locked safe, draw or cupboard, or a similarly secured location.
- 8.4 Users in possession of AFTRS computers including laptops, notebooks, smartphones and other portable computers that contain Confidential Information must not leave these computers unattended at any time unless the Confidential Information is stored in encrypted form or its access can only be gained using a password.

9 Monitoring

- 9.1 AFTRS reserves the right at any time and without notice to monitor, access, retrieve, copy, read, and/or disclose any files, communications or system information stored or transmitted using AFTRS' ICT Resources.
- 9.2 All files and messages stored on AFTRS systems are routinely copied to tape, disk and other storage media. Information stored on AFTRS systems - even if it has been specifically deleted - is often recoverable at a later date to be examined and where relevant, subpoenaed.
- 9.3 Access to all websites is recorded in the proxy log generated by the proxy server and all information technology actions are routinely logged.

10 Breaches

- 10.1 All suspect policy violations, system intrusions, virus infestations, and other conditions that might jeopardise AFTRS information and AFTRS information and communications systems must be immediately reported to the Director of Technology and Infrastructure or the Head, ICT and Services. These violations, intrusions, infestations and other conditions include but are not limited to:
 - Suspicion that sensitive AFTRS information is, or is suspected of being, lost or disclosed to or used by unauthorised parties.
 - Belief that password or other system access control mechanisms are, or are suspected of being, lost, stolen or disclosed.
 - Unusual systems behaviour such as missing files, frequent system crashes, misrouted messages that indicate a potential virus or security problem.

- 10.2 Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.
- 10.3 If a request for information held on AFTRS' computers is received from an external authority in regard to cases of potentially serious, deliberate, and/or criminal breach, the request must be forwarded to the CEO.
- 10.4 Where Users are found to be in breach of this policy, penalties will depend upon the type and severity of the breach. Penalties may range from the loss or restriction of access, to formal disciplinary action.
- 10.5 If a staff member has a suspicion that this policy is being breached through fraudulent activity they should refer to the Fraud Control Policy for guidance on how to report suspected fraud.

11 Legislation & References

- Copyright Act 1968
- Freedom of Information Act 1982
- National Classification Code 2005
- The Commonwealth Sex Discrimination Act 1984
- The Commonwealth Racial Discrimination Act 1975
- The Commonwealth Disability Discrimination Act 1992
- Privacy Act 1988

12 Policy Review

The Director, Technology & Infrastructure, will review this policy annually.