



Australian Government

AFTRS

AFTRS

## Information and Communication Technologies (ICT) User Policy

<b>Responsible Officer</b>	Director of Technology and Infrastructure
<b>Contact Officer</b>	Manager, Media Information Technology Department
<b>Authorisation</b>	Director of Technology and Infrastructure
<b>Effective Date</b>	This policy comes into effect on 9 December 2008 and replaces the IT User Policy dated 1 February 2006.
<b>Associated Documents</b>	AFTRS Code of Conduct (staff and students) Rules, Policies and Procedures for Students – Misconduct Guidelines on Sending Commercial Email Email Etiquette Guidelines Online Security Policy

### 1. Policy Name

Information and Communication Technologies (ICT) User Policy.

### 2. Preamble

This Policy provides the framework for the use and the security of AFTRS' Information and Communication Technologies (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**

### **i. Information Communication Technologies**

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 servers. It extends to all current, emerging and future ICTs.

### **ii. 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:

- i. AFTRS will provide information and communication technologies (ICTs) to its staff and students and visitors, on-site and externally, as appropriate and according to need.
- ii. 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.
- iii. 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.
- iv. AFTRS may disclose electronic communications, records and other transactions to the appropriate authorities if legally required to do so.
- v. 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.

## **7. Conditions of Use**

- i. 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 manner.
- ii. Users must not use AFTRS' ICT Resources to collect, use or disclose personal information in any way that breaches the Privacy Act 1988.
- iii. Users must not use AFTRS' ICT Resources to copy, download and/or store, burn, transfer and copyright material including software, files containing images, artistic work, live pictures or graphics, computer games, and film and

music and video files that are not licensed and that will place them in breach of the Copyright Act, 1968.

- iv. All content developed and stored on AFTRS' ICT Resources is owned by AFTRS.
- v. Users cannot use ICT Resources for private business activities. 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
  - 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.
- vi. Users are required to use their User-ID to use AFTRS' ICT Resources. Users are not to access the ICT resources anonymously or by false identity.
- vii. 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.
- viii. 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.
- ix. No software can be loaded onto any AFTRS computer system without the prior approval of the Manager, Media Information Technology (MIT) Department or the Director, Technology and Infrastructure. All non-text 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.
- x. Computer systems provided by AFTRS must not be altered or added to in any way without the prior approval of the Manager, MIT Department or the Director, Infrastructure and Technology.
- xi. 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.
- xii. With the exception of users given prior approval by the Director of Technology and Infrastructure, Users may not establish Internet or other external network connections that could allow non-AFTRS users to gain access to AFTRS systems and information. These connections include but are not limited to the establishment of multi-computer file systems, Internet web pages, and File Transfer Protocol (FTP) servers. Users are prohibited from establishing dial-up connections, using modems or other such apparatus, from within any AFTRS premises. All in-bound connections to AFTRS' computers from external networks must be protected with an approved password or ID access control system.
- xiii. Users must not copy software provided by AFTRS without written permission from the Director of Technology and Infrastructure.

- xiv. 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 Manager, MIT Department. If the equipment has been damaged, lost, stolen, borrowed or is otherwise unavailable for normal activities, the custodian must promptly inform the Manager, MIT Department or the Director, Technology and Infrastructure.
- xv. Only AFTRS computers may be used to access the AFTRS network. If users need to bring in their own computer they must first get approval from the Manager, MIT Department or the Director, Technology and Infrastructure.
- xvi. 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, the Student Centre or departmental heads who will forward their recommendation to the Manager, MIT Department or the Director, Technology and Infrastructure.
- xvii. Users should not bring their home computers into the office to process AFTRS information without prior approval from the Manager, MIT Department or Director, Technology and Infrastructure.

## **8. Security Privacy and Confidentiality**

- i. 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.
- ii. All emails and all other communications transmitted and stored on AFTRS' ICT Resources are regarded as official records. AFTRS may inspect or provide copies of electronic communications when investigating possible misuse of ICT resources or if legally required to do so.
- iii. Every electronic document designated as 'Confidential' must display the Confidential marking on the first screen shown to the user. All hardcopy computer output 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.
- iv. Users in possession of AFTRS computers including laptops, notebooks, palmtops 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**

- i. From the date that a User agrees to comply with the IT Policy, AFTRS reserves the right at any time and without notice to monitor, access, retrieve, read, and/or disclose employee communications or system information when:

- a legitimate business need exists that cannot be satisfied by other means
  - the relevant User is unavailable and timing is critical to the activity
  - there is reasonable cause to suspect criminal activity or policy violation
  - monitoring is required by law, regulation or third party agreement.
- ii. 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.
  - iii. Access to all websites is recorded in the proxy log generated by the proxy server and all information technology actions are routinely logged.
  - iv. Electronic messages or files cannot be accessed or disclosed unless on the instruction of two of the following: the Chair of Council or the CEO or a member of the Executive where at least one is the Chair of Council, the CEO or the Director of Technology and Infrastructure.
  - v. Users may not assist others to access or disclose the content of electronic messages or files unless on the instruction of two of the following: the Chair of Council or the CEO or a member of the Executive where at least one is the Chair of Council, the CEO or the Director of Technology and Infrastructure.

## **10. BREACHES**

- i. All suspect policy violations, system intrusions, virus infestations, and other conditions which might jeopardise AFTRS information and AFTRS information and communication systems must be immediately reported to the Director of Technology and Infrastructure or the Manager, MIT Department. 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 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 potential virus or security problem.
- ii. Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.
- iii. 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.
- iv. 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.
- v. AFTRS reserves the right to remove any material it views as offensive or potentially illegal from its systems.

- vi. AFTRS reserves the right to delete, summarise or edit any information posted to AFTRS computers and/or communication systems.
- vii. AFTRS reserves the right to revoke the system privileges of any User at any time.

## **11. LEGISLATION AND 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