Table of Contents **Page**

Introduction

1. This policy sets out policy and guidelines on the use of AAT IT facilities and considerations that members and staff should bear in mind in relation to the use of those facilities.

2. Members and staff must ensure that they understand this policy and the codes of conduct that apply to members and staff, and must ensure that their use of the IT facilities is consistent with relevant policies.

Definitions

3. **IT facilities** means information technology facilities and includes internet, intranet, email, telephones, facsimile, desktop computers, infrastructure, hardware, software applications, printers, photocopiers, recording equipment, audio visual equipment and disk or other storage.

4. **Members and staff** includes all persons who may use the AAT's IT facilities including members, ongoing and non-ongoing employees, agency staff, contractors, consultants, work experience placements and service providers.

IT facilities

5. The IT facilities are provided to optimise the productive capacity of members and staff, which in turn contributes to the achievement of the AAT's strategic objectives.

6. Information technology is an essential tool in the operations of the AAT. These systems record key information about AAT cases, support administrative functions, and permit access to information resources that help members and staff in their work. The IT facilities are essential to daily operations of the AAT and must be used, managed and

protected to avoid breaches of security and disruptions to services. The desktop computer facilities include a wide range of up-to-date software applications (e.g. Word, Excel, etc.) which are essential to our operations.

7. A wide range of other IT services and office machines are provided as tools for productive business purposes.

8. Electronic communications and messages may be Commonwealth records and any such records must be managed in accordance with the Archives Act 1983. They are also subject to other legislation such as the Freedom of Information Act 1982, the Privacy Act 1988, the Crimes Act 1914, the Criminal Code Act 1995 and the Evidence Act 1995. Electronic records and documents are 'documents' for the purposes of most legislation.

9. All electronic communications and information created, sent or received using AAT IT facilities become and remain the property of the AAT and may be accessed by authorised persons at any time.

10. The IT facilities must not be used in any way that breaches generally-accepted ethical standards, brings discredit on the AAT, results in the unauthorised disclosure of information, inappropriately engages with applicants or other stakeholders or jeopardises security.

11. The creation and distribution of digital multi-media material (such as sound recordings and video) has increased significantly in the last few years. Issues related to the use of such materials include a significant use of disk space, a significant load on telecommunications bandwidth, a potential increase in ISP usage charges and the potential to infringe copyright.

Making public comment

12. Members and staff may only make public comment in an official capacity with the express written approval of the President or Registrar.

13. Members and staff may make public comment in an unofficial capacity when making public comment and participating online but should take appropriate measures to indicate that the expressed views are their own.

14. There are implications to the reputation of the AAT when members and staff use the internet, send electronic messages, participate online, engage in social media or give out email addresses or telephone or fax numbers. A particular use may imply an endorsement or authority by the AAT which is not intended or which is not appropriate. (Note: Electronic communications sent using the AAT IT facilities will most likely be identifiable as having been sent from the AAT in the coding of a message).

Inappropriate use of IT facilities

15. While the appropriateness of use of the IT facilities is often a matter of judgment, there are clear instances of unacceptable use (e.g. criminal, politically extremist, pornographic or other offensive material). Activities which are not permitted include:

    a. visiting internet sites or sending, posting, downloading, sharing, photocopying or printing politically extremist, pornographic or other offensive material

    b. visiting internet sites or sending, posting, downloading, sharing, photocopying or printing text or graphics files which contravene the APS and member codes of conduct or exceed the bounds of generally accepted standards of good taste, ethics and workplace behaviour, other than where there is a specific work requirement to do so

c. engaging in any illegal activity, including breach of copyright obligations or downloading or distributing unauthorised software or violating software licences, copyright laws or other laws regarding intellectual property

d. downloading program, music or video files (e.g. MP3s) from the internet without IT approval

e. engaging in any for-profit activity, including, but not limited to, offering merchandise or services for sale

f. engaging in any non-AAT commercial business or any gambling activities (other than e.g. social club raffles, Melbourne Cup sweeps or footy tipping competitions that have been permitted by the Registrar)

g. any act resulting in the unauthorised access to or disclosure of information (e.g. accessing case or applicant records without a business reason for doing so)

h. making, without written authorisation, public comment on political or social issues, including government policy, including by participating in on-line chat sessions, forums etc.

i. sending offensive joke emails or attachments to other persons

j. making defamatory or abusive comments

k. harassing or offending any other person

l. any act or omission which could compromise the security of any computer owned by, or operated on behalf of the AAT, the Australian Government, an internet provider or other person

m. representing to be someone else when sending electronic communications or posting information to an internet site, or sending or posting anonymous messages.

16. External sources such as portable media, CDs, DVDs, mobile and storage devices must be scanned for viruses using the anti-virus software installed on each desktop to prevent inadvertently infecting the network before any files are loaded onto the network. Once scanned and cleared, the files can be opened using the IT facilities. Any files that are identified by the anti-virus software as being infected must be referred to IT section staff to assist in their removal.

17. Only devices approved for use in writing by the IT Director may be connected to the AAT network. Synchronising of devices not provided by the AAT is not supported by the IT section.

18. Members and staff must not take AAT information outside the AAT network, including sending information to a personal email address, unless specific prior written approval is provided through the 'Taking Work Outside the Office' policy.

19. The AAT may be held liable and may be penalised for having unlicensed software installed on any part of the network. Members and staff must not install unlicensed software onto any computer or network device. Unlicensed software will be removed without notice or consultation.

20. AAT systems create audit logs, security event records, access attempt logs and usage records. These logs record details of transactions and who made them. These logs are reviewed by IT staff, managers and auditors on a regular basis to identify unusual transactions or activities. Apparent incidents or possible concerns may be referred to the individual for explanation, to the relevant manager or Senior Member for follow up, or

may be referred internally or externally, which may lead to informal or formal investigation and possible disciplinary action.

21. Usage monitoring of the IT facilities generally takes the following forms:

    a. system level monitoring to ensure system performance and control costs;

    b. security event logs of access to PCs, the network and individual systems;

    c. audit logs of transactions in systems including the username, PC address, date, time and detail;

    d. periodic audits of a small number of accounts selected randomly to ensure compliance with usage and storage policies;

    e. review and analysis of specific usage records, or ongoing monitoring of particular accounts in response to a specific enquiry, complaint or investigation; and

    f. automated monitoring of visits to inappropriate sites or transmission or storage of inappropriate materials.

22. Members and staff should be aware that all IT activities may be logged and stored. As well as actual content, the date and time of transmission and receipt, and the addresses of the sender and recipients may be recorded. The addresses of internet sites visited, the date and time they were visited and the duration of site visits may be logged. The AAT have the capacity to recover evidence of inappropriate usage, even when such evidence has been 'deleted'.

23. The AAT reserves the right to censor any electronic messages. Electronic messages sent or received by members and staff may be intercepted by authorised IT personnel. For example, an email containing spam or sexually explicit content sent by one person to another person may be intercepted by an email security mechanism before receipt by the intended recipient.

24. The purpose of these controls is to assist in maintaining the security of the AAT IT facilities and preventing unauthorised access to, or inappropriate use of the IT facilities. The controls also minimise the risk of a potential liability arising as a result of illegal, improper or offensive activities being undertaken through the IT facilities.

25. Access to telephone, fax and proximity card logs, and the logs and content of emails and browsing activities is strictly controlled and limited to particular authorised IT employees. The Registrar may authorise IT to provide copies of a person's logs or emails to that person's supervisor or more senior manager, or to a person conducting a formal investigation. In these circumstances, the material would be provided on a strict 'need to know' basis and would only cover instances relating to a potential breach of the guidelines, other policies, or actions inconsistent with applicable codes of conduct.

26. Authorised IT staff must keep a record of any access or changes to staff or member logs, email accounts, network accounts, secure network drives or any other information store in the form of a record in the IT Support database and email notification to the Director, IT. IT staff must not access any information they are not authorised to access or that is not required to be accessed in the course of their duties.

27. Authorised IT employees may be required to access logs, emails, faxes and computer files or to monitor activities as directed by the Director IT, Registrar or Division Registrar when:

    a. there is a concern that the safety or well-being of a person may be threatened;

    b. there is a need to identify information to respond to a FOI request;

    c. an internal or external complaint is received;

d. the information is required for the AAT to conduct its operations;

e. access is authorised as part of an investigation by the police or an external agency;

f. there is a need to investigate system performance problems; or

g. misuse of the IT facilities is suspected.

Blocked internet sites

28. The AAT use internet monitoring software which blocks access to certain sites in certain categories. Sites may be blocked for a number of reasons including inappropriate content, bandwidth usage, security risks, downloads, irrelevance and time wasting. The AAT may add or remove sites to these lists of blocked sites at any time. It is recognised that at times some members and staff may have valid business reasons to access in the course of their work internet sites which contain disturbing content - such as content related to torture and trauma, extreme political views or other material. Members and staff may gain temporary access to a blocked site for work purposes with written approval (in email form) from their EL2 Manager, Senior Member, Director IT, Registrar or Division Registrar.

Copyright

29. Breaches of copyright may expose both the AAT and individuals to prosecution. Members and staff must ensure that all information stored, copied, or transmitted has been legally obtained and that subsequent use of that information complies with the Copyright Act 1968. Websites often state what is permitted or not permitted in relation to material on a site. If there is not statement about copyright on a website it may be implied that material can be printed or downloaded. Distribution of the material is another matter, and it is recommended that the addresses of websites should be communicated rather than the content in such circumstances.

Personal use of IT facilities

30. The AAT wish to support members and staff in achieving a balance between work, family and other outside interests. Limited personal use of IT facilities is permitted, provided that it does not impact on the functions, business or reputation of the AAT or the security of IT facilities, and where it is a negligible use of time and resources. This may include limited use of telephones, email, fax facilities, scanners, printers, photocopiers and the internet (including for personal account transactions).

31. All members and staff should be cautious in using their work email address for private purposes. Work email addresses should not be used to register on any commercial or other sites that could potentially be damaging to the AAT's reputation, such as dating or gambling websites.

32. AAT IT staff are not required to provide support to any non-standard, non-work related devices or applications or solving access issues to an internet site where no AAT-related purpose is identified.

33. The AAT cannot guarantee the security or privacy of communications. The AAT is not responsible for any loss to members or staff resulting from the private use of the IT facilities.

34. Personal use of IT facilities should be confined to times where there will be no impact on work responsibilities, for example during lunch and before and after normal office hours or in a break agreed with the manager or supervisor.

35. Stored personal material should not exceed 150Mb in total per individual and must only be stored in the computer folder referred to as ‘My Documents’ or ‘H: drive’, or in an email folder clearly titled to indicate that it is personal email material.

36. Managers or supervisors may restrict both the frequency and duration of private use of IT facilities because of operational or system requirements or limitations, in relation to performance management arrangements, bandwidth and network performance issues or in relation to reducing health and safety risks.

37. Members and staff should not use personal accounts for business purposes.

Compliance

38. The Public Service Act 1999 provides that the use of Commonwealth resources must be undertaken in a proper manner. Staff must behave in a manner which upholds the Australian Public Service Values, complies with the APS Code of Conduct and maintains the integrity and good reputation of the employee’s Agency and the APS, in respect of which this policy provides specific guidance.

39. Improper use of the IT facilities can have an adverse impact on others in the workplace, can cause the AAT to suffer loss, can adversely affect the reputation of the AAT, and can expose the AAT to potentially costly litigation.

40. Breach of these policies may result in a range of sanctions or actions, from a need for training or counselling in the appropriate use of resources, to restricting email and internet access, to disciplinary action in relation to a breach of the code of conduct, to the referral of any illegal activity to appropriate authorities.

41. If a person uses the IT facilities contrary to this policy and is subject to disciplinary or legal action, the AAT will not pay the person’s legal costs or any damages or penalties awarded against the person. If proceedings were also brought against the AAT, the AAT may seek to recover any legal costs or any damages or penalties from the person.

Green ICT (Information Communications and Technology)

42. Consideration should be given to the consumption of power and IT related materials including paper and printer toner.

43. Computers and monitors and other equipment should be powered off at the end of each business day.

User access management

44. Access to AAT IT systems must be requested and authorised in writing using the Access to AAT Systems and Premises form available on the AAT Intranet. The Access to AAT Systems and Premises form requires the authorising manager to specify the type and level of systems access required. The level of access must reflect the duties and responsibilities of the new user.

45. Access to computer systems for new staff must be authorised by the relevant Executive Level manager using the Access to AAT Systems and Premises Form. New members are authorised by the Director IT, Senior Members, Division Registrar or Registrar. Where a new user is a non-ongoing employee, temp, or consultant, the end date of their engagement must be specified. Subsequent extensions of systems access may then be notified to IT by email if the engagement is extended.

Modifying user access

46. Staff movements and changing job roles often require different, additional or higher level systems access. Managers should advise IT of staff movements in writing. Requests to change user access may be made via the staff movement or access request form. Where the access change is related to temporary transfer or Higher Duties temporary transfer, an end date must be specified. The end date must be the same as the end date of the temporary transfer or Higher Duties temporary transfer.

47. IT staff periodically review user access levels with business owners to confirm the validity and appropriateness of user access to ensure that access privileges are consistent with the day to day requirements of the user. Changes to restricted functions and some data are notified immediately to business systems owners.

Suspending user access

48. User accounts will be suspended for any absence from duty exceeding 4 weeks, including leave or temporary transfer, on notification to the IT team. Managers and Human Resources must notify IT of extended absences.

Terminating user access

49. When a user leaves the AAT, an “Exit checklist” must be completed to ensure that systems access can be terminated and data can be removed.

50. Managers and Senior Members must ensure that departing members and staff transfer data, documents and emails which are corporate records prior to separation. Paper records must be placed on the relevant case files or policy files, and electronic copies of emails and documents which are relevant to current activities must be placed in common drive or team folder on the network, or handed over to the relevant Manager or Senior Member in a suitable format, such as a CD-ROM/DVD.

51. Where there is a possibility of a disgruntled person misusing, damaging or destroying data, managers and Senior Members should advise IT immediately so that user access may be restricted or terminated.

System administration

52. Administrator privileges for the network will be held only by IT staff. IT staff must use their separate administrator accounts to use administrative privileges. Changes to default user settings by IT staff are not permitted.

53. Business owners of systems may be given administrative access to their own systems for a specific period or purpose. Non-IT members and staff with administrator privileges are restricted to using those privileges only for the purposes for which they were granted.

54. Business owners of systems are required to review access rights for their systems on a monthly basis, confirming the appropriateness of access levels.

55. Requests for administrator privileges may only be approved by the Director, IT or in his/her absence by the Registrar or Division Registrar. Accounts with administrator privileges are reviewed regularly and un-authorised accounts will be closed.

Password security

56. All user accounts are required to adhere to industry standard password rules enforced by the network including regular refresh, adhering to complexity rules and non-disclosure.

57. If a PC is left unattended it must be locked using the CTRL-ALT-DEL facility in Windows. The PC will lock automatically after 15 minutes; the password must be re-entered to unlock it.

58. The IT section will not provide generic accounts with passwords that can be shared.

59. Passwords must be kept securely and not given to anyone. Members and staff must not allow someone else to access AAT computer systems using their account, their details or proximity card. Having a password visible in a work area will be regarded as a serious breach of security.

Additional guidance

60. The Registrar, the Division Registrar or the Director IT may from time to time issue additional guidelines regulating the safe and efficient use of the IT facilities, including but not limited to:

    a. storage limits;

    b. policies for storing and deleting emails;

    c. policies for working from home, taking work outside the office, changes in technology and additional device availability;

    d. correct use of distribution lists, group mailboxes and email public folders;

    e. limiting access to websites or other sources that may have an impact on bandwidth or pose a security, information risk;

    f. avoiding potential breaches to the security of systems and information; and

    g. avoiding attack by malicious software and hackers.

61. Where uncertainties or issues arise, or there are concerns about suspected misuse of the IT facilities, Members and staff should consult the Registrar, the Division Registrar or the Director IT.

Whole of government guidance

62. All members and staff are required to comply with any other directions, guidelines, or policies as advised and provided through other agencies including, but not limited to;

    a. APSC Circular 2012/1: Revisions to the Commission's guidance on making public comment and participating online

    b. b. Attorney General's Protective Security Policy Framework (PSPF) <https://www.protectivesecurity.gov.au/ExecutiveGuidance/Pages/default.aspx>

    c. c. Australian Government Information Management Office (AGIMO) <Email Protective Marking Standard for the Australian Government – September 2011>

    d. d. Defence Signals Directorate (DSD) Information Security Manual <http://www.dsd.gov.au/infosec/ism/index.htm>

Superseded documents

63. This policy replaces AAT Personnel Direction No. 6 – Internet and E-mail Policy

Sian Leathem
Registrar
13 October 2015

Revision History:

Date	Reason for update	Issue no.	Proposed review date.
7 October 2015	Tribunal amalgamation	1.0	September 2017 or earlier if required for operational reasons.