



One Cadet

ADF Cadets ICT Management Protocol

As a supplement to the ADF Cadets ICT Policy, this Management Protocol provides ADF Cadets and Adults with procedures and processes to effectively and securely manage ADF Cadets ICT systems. This document identifies the responsibilities and activities of ADF Cadets Headquarters (ADFCHQ) and the Cadet Organisations to manage ICT systems provided for ADF Cadets.

Effective management and security processes for ADF Cadets information systems

- **Information Security Manager (ITSM).** ADFCHQ will maintain suitability qualified Defence personnel to act as the ITSM for CadetNet. The ITSM will be required to work with CIOG and the Office of the Australian Information Commissioner regarding legislative, regulatory and voluntary notifications concerning security matters with the Cadet Information Environment.
- **Information Technology Security Advisor (ITSA).** Each Cadet Organisation will maintain suitability qualified staff within their headquarters to perform the role of ITSA. The ITSA will work with the ITSM in maintaining security arrangements for CadetNet. They will provide advice to users on security matters pertaining to the use of CadetNet and data contained within the network.
- **Incidents.** Security incidents, including data breaches, are to be reported immediately to the Security Incident Centre using the Security Incident Report form (XP-168 or XP-188).
- **Security Oversight.** Chief Information Officer Group (CIOG) provide security oversight for CadetNet. ADFCHQ is to promptly hand matters raised through the various security team's monitoring the system to the respective Cadet Organisation or vendor for remedial action.

ADF Cadets ICT system development, testing and sustainment

- **CadetOne (C1).** CadetOne has been developed and is maintained by AAFC members to enable their business processes. It is not hosted by Defence however is subject to the same information system, security and privacy requirements as CadetNet (as defined in the relevant legislation and the Information Security Manual (ISM)). AAFC business processes are currently being prepared for transition to CadetNet. It is expected that C1 will be retired in the future once all transition activities have been completed.
- **Account Management.** There is provision for contractors to Defence and approved stakeholders to be granted limited access accounts for specific purposes. Each ADFCHQ can create these as required if the appropriate contract for services is in place with the Defence.





- **Issue Management.** Users must report issues to their ADFCHQ ICT team for resolution via the approved Issue Tracking system. For unit members this will usually be the organisation's ICT tracker accessible through their Intranet on CadetNet.
- **Testing.** Each Cadet Organisation will be responsible for providing members available for testing new system functionality and regression testing as required. This may be conducted remotely from their home or work location, or residential during specified User Acceptance Testing (UAT) activities arranged by ADFCHQ.
- **Outages.** ADFCHQ will advise the Cadet Organisation ICT managers of any scheduled outages and unscheduled outages as soon as practicable. The CadetNet status site (www.cadets.net.au) will be updated before, during and after each event.

ADF Cadets broadband network connections and support

- **Connection Tracking.** A connection tracking collaboration site must be used to track all orders and the status of all Defence provided connections. ADFCHQ, in conjunction with the vendor(s), are to provide high level reports on usage as required.
- **Total Number of Connections.** The ADFCHQ manages the total number of connections in consultation with the Cadet Organisation ICT managers. Additional connections may be considered to be available although will often require additional funding being supplied by the requesting Cadet Organisation.
- **Own Unit Connections.** ADF Cadets units may arrange their own broadband connection and agrees to take full responsibility for the funding, infrastructure, equipment, support and usage of the connection. The relevant ADFCHQ is required to implement and maintain a risk assessment for each location opting for this solution to ensure security, reputation and other risks are appropriately identified and managed appropriately.

ADF Cadets ICT hardware assets

- **Types and Allocation.** ICT assets supplied by Defence to cadet units includes at least one of each of the following:
 - a. standard personal computer and Liquid Crystal Display (LCD) monitor;
 - b. laptop;
 - c. multi-function device (MFD) with print and scan capability;
 - d. data projector; and
 - e. modem/router for broadband internet (note these items are currently supplied through ADF Cadets specific broadband contracts and not CIOG).
- **Management of ICT Assets.** ADFCHQ is to implement appropriate procedures and protocols for ICT hardware, having sourced information from CIOG and appropriate vendors. ADFCHQ is the coordinator for Defence ICT assets on behalf of the ADF Cadets ensuring that a common approach is implemented.
- **Stocktake.** Failure to comply with the stocktake requirements each year will delay the provision of support to faulty equipment and the due date for refresh of assets.
- **Consumables.** ADFCHQ supplies toner cartridges for supported printers on the basis of one per year per unit. Printing ribbons and blank cards for Grey Series identity card printing are also supplied as required.





- **Unit Owned Devices.** In some circumstances Unit Support Committees (USC) or the community may purchase ICT assets for their local unit however these assets are not supported in any way by Defence and the cadet unit (or the Committee) retains sole ownership, and responsibility for the maintenance, repair, refresh and support of these assets for the entirety of their use in the cadet unit.
- **ICT Purchase Register.** To ensure visibility, ADF Cadets must register the purchase of all ICT assets on CadetNet.

ADF Cadets web estate management

- **Internet Sites.** ADFCHQ is responsible for managing all relevant *.gov.au* domains together with the Defence web managers. The use of other domains (including those ending in *.com.au* and *.org.au*) are not to be used for official ADF Cadet sites. The use of *aafc.org.au* by the AAFC is an exception until business processes including web hosting are migrated into the CadetNet environment. All official sites are to use the approved Defence banner and refer to the Defence privacy, freedom of information and copyright statements in the footer.
- **Independent Internet Sites.** ADF Cadets members and DAH are not permitted to create their own internet based web site relating to their ADF Cadets involvement, nor are they permitted to publish unapproved content to existing sites either Defence maintained or otherwise.
- **Unit Directory.** ADFCHQ is responsible for maintaining a publicly accessible unit directory with contact information updated by the ADF Cadets.
- **Intranet.** Each Cadet Organisation maintains their respective intranet presence hosted on CadetNet. Each ADFCHQ, units and project groups may have their own intranet information or collaboration site for members to access and contribute as required. ADF Cadets members are not permitted to create their own member's areas outside of CadetNet.

Further information

This guide should be read in conjunction with the ADF Cadets ICT Policy. For further information on CadetNet please log on at www.cadetnet.gov.au.

