ICT Asset Management

Policy
A comprehensive program to monitor the location, use and value of all Information and Communications Technology (ICT) equipment and facilities will be established and maintained.

Policy Guidelines

1. Assets Register - Physical and Logical Assets
Each physical asset and all logical assets, comprising packaged software and developed application systems will be identified and recorded in an Asset Register which is regularly maintained.

2. Inventory Review - Physical Assets
A stock-take of all ICT physical assets will be undertaken annually, and all discrepancies reconciled.

3. Appropriate Use
Staff must be conscientious in the business use of DECD information systems and facilities. All use must comply with policies relating to the internet, email and acceptable use.

4. Personal Use
DECD staff are permitted reasonable personal use of the site DECD ICT facilities and software as long as that use does not compromise or impact the security of those facilities, DECD information systems and DECD information and does not conflict with the Commissioner for Public Employment’s Code of Ethics and DECD policies and standards. Portable PCs and other computing equipment which is used outside the office environment is subject to security controls, over and above those which apply within the DECD environment, to recognise the increased risk involved.

Staff must log out the ICT items that they wish to borrow in the Log book provided by the sign in/out sheet with name, item, date taken and returned and co-signed by the Director.

5. Unauthorised Equipment or Software
Unauthorised equipment and unauthorised or unlicensed software must not be installed on, attached to or operated on any DECD ICT facilities. Any equipment or software identified as unapproved and/or unlicensed must be removed immediately.

6. References
The following whole-of-government policies and DECD policies are relevant and must be read in conjunction with this policy.
- DECD Policy - ICT Security
- DECD Policy - Internet Access and Use
- DECD Policy - Email Access and Use
- DECD Standard - Corporate Managed Desktop Environment
- Information Technology Infrastructure Services Policy
- Telecommunications Services Policy
- Personal Computers Policy
- Microsoft Software - MS Select Program Policy
- ICT Infrastructure Standards Policy

7. Acceptable Use Policies
DECD staff must use ICT resources in an appropriate and professional manner according to the Code of Conduct published by Commissioner for Public Employment. Acceptable use policies must be in place for all users, including staff and students. Such policies must be in the form of a written agreement, signed by staff outlining the terms and conditions of use of DECD ICT facilities, and of online behaviour and access privileges, and consequences of non-compliance.
8. **Access Control and Management**
*Users must only be supplied with the level of access required to perform their work duties. Users must not attempt to gain access beyond their given access privileges.*
*An effective access control system must be provided and properly maintained over all DECD information assets according to their classification. No user shall bypass any security controls without the approval of the Preschool Director.*
*All security and access privilege requests, establishment, change and removal must be logged to an audit trail to allow subsequent review.*

9. **User Identification**
*Users of DECD computer systems must be identified by a unique user identifier (user-id).*
*The use of shared group user-ids will only be used in special circumstances, and only after approval from the Preschool Director.*
*Personal user-ids must not be shared between people.*
*All user-ids must be protected by a secure password or other approved mechanism.*
*All users will be accountable for any actions undertaken by their personal user-id.*

10. **Passwords**
*Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information (e.g. names, telephone numbers of dates of birth).*
*Passwords must be kept confidential and not displayed or written down in any form.*
*Users must change passwords at regular intervals, based on the classification of the information being protected, and whenever there is an indication of possible system or password compromise. *Systems should require users to change initial passwords at their first log on.*
*Passwords must not be included in log on scripts or other automated log on processes.*
*Users must not disclose their personal password to any other person. Where users are authorised to use group user-ids, the password must not be disclosed to unauthorised people.*

11. **Information Transport, Storage and Transmission**
*Adequate security must be maintained over information during transport and storage, whether in electronic or non-electronic form, to ensure there is no unauthorised disclosure or damage.*
*The risks and consequences of unauthorised or accidental release of sensitive or confidential information must be assessed when transmitting information by facsimile, email or any other insecure means.*

At the end of the working day, all portable ICT assets must be stored in the Confidential Children’s File Cupboard in the kitchen and secured before leaving. This includes the I Pad, Cameras, Lap top computer and mobile phone. Both photocopiers must be covered.

12. **Removal of DECD Property**
DECD ICT equipment, information or software must not be taken off-site without appropriate authorisation. Where appropriate, removal and subsequent return of DECD property should be logged. Adequate security must be maintained over information during transport and storage, whether in electronic or non-electronic form, to ensure there is no unauthorised disclosure or damage.

13. **Staff Induction**
All new permanent and temporary employees, consultants and contractors engaged by DECD must be provided with training and appropriate documentation about the requirements of DECD ICT security policies.

14. **User Training**
All users of DECD ICT facilities must be provided with appropriate security awareness training. This training will minimise ICT security risks and ensure that users are equipped to support DECD ICT security policies in the course of their use of DECD ICT facilities. User awareness will be supported by staff Induction Process at the beginning of the year.

15. **Definitions**
In the context of this policy:
*‘confidentiality’ means ensuring that information is only available to those authorised to have access.*
*‘integrity’ means safeguarding the accuracy and completeness of information and software.*
*‘availability’ means ensuring that information and vital ICT services are available when required.*
*The term ‘user’ includes any person granted access to the site DECD ICT facilities or services. This includes site staff and special needs team personnel.*
*The term ‘information asset’ means any data or information, as well as related equipment that contains or processes data or information, that is relevant to DECD functions.*
The use of DECD ICT resources is governed by DECD and Government policies. These policies are in place to protect DECD information assets from a range of threats including loss, corruption, disclosure, theft and interruption of services.

This user agreement applies to all staff (which includes contractors and temporary employees), who have computer access at DECD corporate sites, and is to be completed by all users before they are given access to DECD ICT facilities.

The signed form must be retained by the DECD Authorising Officer.

IMPORTANT: you must read and understand the documents and policies referenced in this user Agreement, Refer to DECD web site to view all policies and documents.

Users of DECD ICT facilities must:
1. Understand and adhere to the requirements of the DECD Policy - ICT Security, which is published on the DECD intranet.
2. Use DECD ICT facilities in an appropriate and professional manner according to the Code of Ethics published by the Commissioner for Public Employment.
3. Understand and adhere to the requirements of the DECD Policy - Internet Access and Use and the DECD Policy - Email Access and Use, both published on the DECD intranet.
4. Follow the directions of ICT Service Desk relating to their use of DECD ICT facilities.
5. Specifically, the access, transmission, retrieval, storage and/or display of:
   - sexually explicit material;
   - hate speech or offensive material;
   - material regarding illicit drugs or violence;
   - material regarding criminal skills and/or illegal activities;
   - material of a defamatory, discriminatory or harassing nature;

is strictly forbidden if that material does not form part of a legitimate educational inquiry.

Violations of this policy, depending on severity and nature, may result in reprimand, loss of ICT access privileges, termination of employment or any other appropriate disciplinary action.

USER DECLARATION
By using DECD ICT facilities I acknowledge and agree to the above terms and conditions. I have read and understood the requirements of the:

- DECD Policy - ICT Security;
- DECD Policy - Internet Access and Use;
- DECD Policy - Email Access and Use.

I undertake to ensure that my PASSWORD is kept confidential, and acknowledge that unauthorised use of my personal USER ID may result in the integrity of the system being compromised. I further accept that I am responsible for ensuring my personal USER ID is not shared and is only used for proper and authorised activities, and am accountable for any actions undertaken using my USER ID.

I also understand that DECD/DTEI monitors email and Internet activity undertaken by users who have access to resources provided by DECD.

I have read and understand this user agreement and I will observe and be bound by its conditions at all times.

Signature: Name: Date: