1. **POLICY STATEMENT**

1.1 This policy details the security requirements relating to portable devices which connect to the Education and Training Directorate’s IT networks within schools.

2. **RATIONALE**

2.1 The Education and Training Directorate has developed this policy as a result of the increasing use of these devices, and the significant potential threat these devices have for Corporate Data.

2.2 The underlying principle is that all devices, including privately owned devices, used to hold and/or process school related information, must be given the same level of security and protection as the information stored on them. It is understood that the bulk of information stored on portable devices is not IN-CONFIDENCE, PROTECTED or business critical information, however staff must take reasonable care to protect the device and any information stored there-on.

3. **DEFINITIONS**

3.1 **Device**: in the context of this policy a device is any portable media which has the capability to store information.

Types of devices include:

**PDSD** (Portable Digital Storage Device): is the element of hardware that is used to store information (also known as Removable Media)

PDSDs include but are not limited to:

- External Hard Drives
- DVD’s
- Compact Disks (CD’s)
- Floppy Disks
- Tapes
• Smart cards
• Flashcards
• USB Drives.

**PED (Portable Electronic Device):** portable devices that can store, access process and / or transmit information electronically.

PEDs include, but are not limited to:

• Mobile telephones
• Two-way pagers
• Digital cameras
• Audio recorders
• PDAs (Personal Digital Assistant).

A portable electronic device is generally differentiated from a portable computer by its inability to have comprehensive security features, including user identification, authentication, and auditing.

3.2 **UNCLASSIFIED:** constitutes the bulk of information in a school, e.g. teacher working documents.

3.3 **X-IN-CONFIDENCE:** information which could potentially harm the government, commercial entities or members of the public. For example, in the school sense this classification would apply to information which links student names to home addresses and/or home telephone numbers.

3.4 **PROTECTED:** information which if compromised could endanger individuals or private entities. Very little information would be classified at this level in a school.

4. **PROCEDURES**

**Care and Storage**

4.1 A clean desk policy applies to departmental staff regarding the visibility of portable devices. These devices should be kept out of sight at all times unless the device is being used for a specific purpose. This is to minimise the risk of theft, and reduce the risk of the device being damaged or destroyed either by fire, flood or accident.

4.2 Portable devices, which store PROTECTED or business critical information, must be recorded in the school’s, or section’s, ‘Portable and Attractive Items’ register.

4.3 The information contained on portable devices should be frequently backed up to the EDUnet server for protection against loss or damage.

**Transport**

4.4 Devices holding corporate data must be handled in the same way as paper documents of the same classification during transportation.
4.5 Care must be taken to prevent portable devices being subjected to heat, water or magnetism at any time. Data may be corrupted or rendered unreadable. If this occurs beyond repair, the device must still be appropriately sanitised and disposed of.

Cleaning/Sanitisation

4.6 Compact Disks and DVDs cannot be appropriately sanitised by media overwrite, and they must be destroyed either by an approved disintegrater, or by grinding, smashing or burning.

Disposal

4.7 After a portable device has been sanitised, it may then be disposed of. Please refer to the Fact Sheets section on Index on Disposal of Media for further instructions. Refer to the Fact Sheets section on the staff intranet on Cleansing/Sanitisation of Media for further instruction of how to sanitise a PDA.

Lost or stolen devices

4.8 If a directorate portable device is lost or stolen, it must be reported to the IT Service Desk within 12 hours from the time it was noticed missing. The IT Service Desk must be notified of the asset number of the device, a description of the device, details of the loss/theft and what information was kept on the device. Please refer to the Incident Report Form found on the staff intranet, Index, to be submitted to the IT Service Desk. The form supplied by Facilities section if hardware is lost or stolen must also be completed.

4.9 The Data Integrity Unit will assess the impact of the situation and follow up according to the risk.

5. Guidelines

5.1 Devices covered by this policy:

- must be protected in accordance with the requirements for the storage of similarly classified hardcopy material that is consistent with the requirement of the Territory Records Act (2002) associated standards, guidelines, and advice
- must have the most up-to-date anti-virus software and security patches
- can be connected to the Edunet network, including privately owned devices, but are NOT to be used to store any information classified at 'X'-IN-CONFIDENCE and above. Student names together with an identifying address or contact number is an example of data that would be classified at 'X'-INCONFIDENCE. An exception is when the portable device has been encrypted and it may then be used to store data at higher classifications. Normal student reports, timetables and other working documents would be viewed as being unclassified
must not be shared by staff with other directorate employees unless the employee has specific rights to view the stored data at that level of classification. Portable devices holding department information cannot be shared with people outside of the directorate. This includes privately owned portable devices

PDAs and Smart Phones in particular must not store information classified at ‘X’-IN-CONFIDENCE or above unless the device is encrypted. If the device synchronises with a user’s Inbox, then that user must ensure that the PDA is not downloading information at that classification. This can be overcome by archiving sensitive email before synchronisation occurs. PDAs must also have password protection in place to ensure information stored on the device has some protection if it is lost or stolen. The Data Integrity Unit will provide assistance if required.

5.2 The highest classification level of most information held by schools is ‘X’-IN-CONFIDENCE. There are occasions when information about staff and students could be classified as PROTECTED. In these instances such information should only be stored on the department’s EDUnet servers and not stored or transported on a portable device unless encrypted.

5.3 Schools should:

- house all devices covered under this policy, that store or may store departmental information, data or records, in a secure area to protect against theft and to limit access
- remind students of the need to protect their personal devices and the data stored on them.

References


Draft ACT Protective Security and Guidelines Manual, developed by the Justice and Community Safety Directorate, in conjunction with the Chief Minister and Cabinet Directorate

Related Policies:

IT Security Policy
Acceptable Use of Computer Facilities and External Networks Policy (the policy on the Appropriate Use of Portable Digital Storage Devices, Removable Media and Non-Corporate Drives will complement this policy).
School Developed Acceptable Use IT Security Policies and Statements. Director-General's Financial Instruction, 6.1 'Asset Management'

This policy is based on the provisions of the 'Australian Communications – Electronic Security Instructions 33 (ACSI 33)' and 'AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management.'