POLICY TITLE:	**SENSITIVE INFORMATION HANDLING POLICY**
YEAR OF PUBLICATION:	2007
IDENTIFIER:	SIH200703
LEGISLATION:	*Territory Records Act 2002* *Privacy Act 1988 (Commonwealth)* *Criminal Code 2002* *Crimes (Offences Against the Government) Act 1989* *Freedom of Information Act 1989* *Executive Documents Release Act 2001* *Public Sector Management Act 1994* *Electronic Transactions Act 2001* *ACSI 33 Australian Government Information & Communication* *Health Records (Privacy and Access) Act 1997* *Commonwealth Protective Security Manual (PSM)*

1. Policy Statement

1.1 Access to sensitive information must be strictly limited.

1.2 Sensitive information must be stored securely at all times.

1.3 Employees should have access only to the sensitive information needed to complete their duties.

1.4 All levels of management are accountable for the security of all sensitive information under their control.

1.5 System access and other access tokens must be immediately removed when employees discontinue their employment with the Department.

1.6 Copies of sensitive information must be treated with the same standards of protection as the original document.

2. Rationale

2.1 This policy aims to ensure that the Department of Education and Training meets its legislative requirements in managing all sensitive information it holds.

2.2 Departmental officers need to be aware of their responsibilities in relation to handling, storing, accessing, disposing, using and disclosing sensitive information.

3. Definitions

Information:
Refers to any form of information including:

- documents and papers
- electronic data
- the intellectual information (knowledge) acquired by individuals
- physical items from which information regarding design, components or use could be derived
- photograph or other pictorial representation of a person.

Records:
Information made, received, and maintained as evidence and information by an agency or person, in pursuance of legal obligations or in the transaction of business. This recorded information must be maintained or managed by the agency to provide evidence of their business activities. Records can be written, electronic or any other form.

Sensitive Information:
There are different types of sensitive information. These include but are not limited to:

- personal information (e.g. criminal, health, welfare, personnel records)
- student records and other student information
- information relating to counselling and working with children and young people
- financial or commercially sensitive information (e.g. budget, tender information)
- information given in confidence
- information relating to an investigation (e.g. malpractice, discipline, complaint records)
- information posing a security risk (e.g. building plans & access codes)
- legal advice.

Sensitive Information Classifications:

- **Cabinet in Confidence** (This marking refers to all Cabinet and related documents, including documents that refer specifically to Cabinet Submissions or Minutes. They must be marked "Cabinet – in-Confidence" at the top and bottom of each page). For further information refer to the ACT Cabinet Handbook.
- **Highly Protected** (This marking indicates that the information requires a substantial degree of protection as compromise of the information could cause **serious damage** to the Territory, Government, commercial entities or members of the public)
- **X - In – Confidence** e.g. Staff-in-Confidence, Commercial-in-Confidence. (This marking indicates when the compromise of information could cause **limited damage** to the Territory, Government, commercial entities or members of the public. This is also accompanied by a notification of the subject matter to ensure correct handling and an easy appreciation of the need-to-know requirement)
- **Protected** (This marking indicates when the compromise of information could cause **damage** to the Territory, Government, commercial entities or members of the public)

4. Procedures

4.1 Sensitive Information Handling

4.1.1 The Department's sensitive information is identified as information whose unauthorised disclosure would damage corporate security or individual privacy, give unfair commercial advantage or cause harm to an individual or organisation.

4.1.2 Special attention must be given to the handling, storage, access and authorisation of such information for use within the Department or for external disclosure. As a general rule, sensitive information must be appropriately marked, dispatched in opaque envelopes, delivered by hand, locked up continuously when not being accessed, not transmitted by fax, not photocopied and be destroyed by a method appropriate to the medium on which the information is stored when the end of the retention period is reached.

4.1.3 All levels of management are accountable for the security of all sensitive information under their control.

4.1.4 As part of their audit responsibilities, all sections in the Department and schools are required to complete the Sensitive Information Register (Attachment A). This register must also be updated on a yearly basis.

4.2 Privacy

4.2.1 The privacy of each person must be recognised and protected as required in the 11 Information Privacy Principles under the Privacy Act 1988 and/or the Health Records (Privacy and Access) Act 1997 Part 2 Privacy Provisions. Personal information must only be collected and used for purposes specified at the time of collection, unless exemptions under privacy legislation apply. It must be accurate, complete and up to date when used. Advice is available from the Governance and Legal Liaison section or from the School Legal Information Manual (SLIM) Module: Privacy, available on "index".

4.2.2 Disposal of information must be in accordance with the Department's Records Management Program. For further information on the destruction of records please contact the Records Management Section.

4.2.3 Legislative safeguards apply for the appropriate collection, use, disclosure, protection and disposal of personnel and student information. Different circumstances may arise e.g. requests for disclosure of information from AFP, Centrelink, OCYFS or Subpoenas. Advice is available from the Governance and Legal Liaison section or from the School Legal Information Manual (SLIM) Module: Privacy, available on "index".

4.2.4 Records containing information about departmental staff and students (including counsellor records) and information about other persons may only be created or accessed by those who have authority to do so.

4.2.5 Paper-based records containing personal information must only be accessed by staff with the appropriate authorisation and who need to know the contents of those files to perform their official duties. When not in use, this information must be securely stored, preferably in a lockable container for which only authorised staff have access to the keys or combination.

4.2.6 When such information must be transferred to other staff at different locations within the Department, they must be inserted into opaque envelopes, marked clearly as "Staff-In-Confidence" and addressed only to those who also have authorisation to access these files. Envelopes must be firmly sealed before being transferred by internal mail or courier service.

4.2.7 Staff must adhere to the Department's Information Technology Security Policy, and the Acceptable Use of IT Resources Statement, available on index, when using information technology resources to manage information and in particular when using email to transmit personal information regarding staff members, students or other individuals. If email is used, the sender must print out these messages and attach hard copies to the appropriate file. Further information can be obtained from Data Integrity Unit.

4.2.8 Staff who have access to the departmental HR system must ensure that sensitive information contained in that system is maintained only for the purposes for which it was collected, is secure from unauthorised access, and retained for the appropriate period as required under the Territory Records Act 2002 and relevant disposal schedules. Details concerning provisions of this act and the required retention period for such records can be obtained from the Records Management Section.

4.2.9 New office and school based staff must be provided with training in the handling of sensitive information as part of their induction. Also refer to Public Sector Management Act 1994 Part 2 Division 2.1 Section 9 General Obligations of Public Employees.

4.3 Physical Security

4.3.1 Sensitive information must be kept secure throughout the day and accessible only to those staff who require access to complete their duties. Unclassified files held in business units should be accessible to all staff who need them but must be secured at the end of the day.

4.3.2 Hard copies of sensitive information must not be removed from the workplace without prior approval and must be kept secure and protected against unauthorised duplication, deletion, modification or theft. If files are kept overnight, or during periods of absence from the office, they must be secured or kept in an area away from public view or access and where there is some form of access control and oversight by staff.

4.3.3 Staff who have access to the Department's Central Records System must ensure that they only mark sensitive records for transfer to other staff entitled to access those files, as they will be accountable for these movements.

4.4 Clear Desk Policy

4.4.1 All departmental staff are responsible for all sensitive information in their custody, including paper files marked out to them. No files should be left lying on desks and loose documents must be kept within a folder. Work areas should always be kept clean and tidy.

4.5 Access

4.5.1 The Department has an obligation to conform with relevant Territory and Commonwealth legislation for controlling access to and handling of sensitive information. Broad policies and practices are detailed in the ACT Protective Security Policy and Guidelines Section 4 – Information Security and the DET

Privacy Statement. (This policy is currently in draft format and cannot be accessed until it has been approved. A link to the relevant section of this policy will be made when this policy is released).

4.5.2 Only those staff members who have a genuine 'need to know' or whose names or their designations appear on a restricted access list should be permitted access to specific records and information. Restricting access on a 'need-to-know' basis assists in reducing the likelihood of unauthorised removal, copying, alteration or compromise of that information.

4.5.3 As a general principle, a staff member has a genuine 'need to know' where, without access, he/she would be hindered in the effective performance of his/her duties. Staff are not entitled to access merely because it would be convenient to know or by virtue of office or level of management.

4.5.4 Sensitive information that is classified as Cabinet in Confidence must be handled in accordance with the current version of the ACT Government Cabinet Handbook, in particular Chapter 7 *Security and Handling of Cabinet Documents* and Chapter 8 *Access to Cabinet Documents.*

4.6 Control

4.6.1 Staff responsible for the custody of confidential information must ensure that the information is stored in areas away from public view or access, and where there is some form of access control and oversight by staff. Electronic documents must be stored in line with the Department's IT security policies.

4.6.2 Factors that will affect the class of security container or secure area required include:

- the level of classification
- the value and attractiveness of the information to be stored
- the location of the information
- the structure and location of the building
- entry control systems
- other physical protection systems (for example, locks and alarms).

4.6.3 Sensitive information may be transferred between authorised staff within the Department either by hand or delivered by an authorised messenger in a sealed, opaque envelope marked "In-Confidence".

4.6.4 Staff members who pass "In-Confidence" confidential records from one section to another must, in their own interests, advise the Records Management Section so they can update the records management system.

4.6.5 If there is a necessity for an area where staff should not be permitted to be left alone a "No Alone Zone" may be implemented by a school or section within the Department. The aim of a No Alone Zone is to enforce "two person integrity" where all actions are witnessed by at least one other person. The No Alone Zone should be:

- suitably signposted
- have all entry and exit points appropriately secured.

4.7 Disclosure of Sensitive Information

4.7.1 Care should be exercised in releasing any personal information to ensure there is no current court order which would prevent this. This is particularly relevant to student information.

4.7.2 A member of the public requesting their own, or their child's information, must do so in writing with proof of identity attached (e.g. current drivers licence). If another person makes the request, a signed authority to release the personal information to that person must also be provided. Proof of identity should again be provided by the person to whom the information is to be released or the requested information forwarded by registered post. The requestor must also be informed that the information they supply will only be used in relation to their original request. All other requests are to be made through the Freedom of Information application process managed by Governance and Legal Liaison section, at http://www.det.act.gov.au/applic/applic.htm

4.7.3 Where parents are seeking personal information of older students who are not yet 18 years old reference should be made to Circular Minute 40/99 "Parents' access to personal information of students", available on "index", or contact Governance and Legal Liaison for advice.

4.7.4 The *Privacy Act 1988* allows for the release of personal information in certain circumstances including where it is authorised or required by law. Refer to School Legal Information Manual (SLIM) Module: Privacy, available on "index" or contact Governance and Legal Liaison section.

4.7.5 Release of health or counselling records can be made under Health Records (Privacy and Access) Act 1997 Part 2 Privacy Provisions legislation. If a request is received for this type of information contact Governance and Legal Liaison for advice.

4.7.6 All sensitive information, including photocopies, must be handled strictly on a 'need-to-know' basis. In order to maintain this standard, photocopying of sensitive information must be limited to essential needs.

4.7.7 Care must be exercised to ensure surplus photocopies of sensitive information are disposed of as 'classified waste' within the 'Normal Administrative Practice' provisions of the Department's Records Management Program.

4.7.8 All sensitive information requests must be in writing and not be provided over the telephone. Refer School Legal Information Manual (SLIM) FAQ 7 page 15, available on "index". MMS (Multimedia Messaging Service) or SMS (Short Message Service) are not to be used to transmit sensitive information.

4.7.9 If sensitive information is to be sent via a fax or mfd (multi function device) the sender must make arrangements for the receiver to:

- collect the information on the fax machine or mfd as soon as possible after the information is received
- notify the sender if the fax does not arrive no longer than ten minutes after it has been sent.

4.7.10 If sensitive information is sent via email, the section must ensure:

- the sending and receiving entities are aware of the risk
- the sending and receiving entities accept the risk

4.7.11 This information should be added if sensitive information is sent by fax or email:

This fax/email is confidential and may also be privileged. If you are not the intended recipient, please notify the sender and delete all copies of this transmission along with any attachments immediately. You should not copy or use it for any purpose, nor disclose its contents to any other person.

4.8 Working from home

4.8.1 No sensitive information is to be stored on home PCs in line with the Department's IT Security policy because the storage is:

- not secure
- not protected against unauthorised duplication, deletion or modification.

4.9 PDSD (Portable Digital Storage Device) storage includes but is not limited to: External Hard Drives, DVDs, Compact Discs (CDs), Floppy Discs, Tapes, Smart Cards, Flash Cards, USB Drives.

4.9.1 No sensitive information is to be stored on PDSDs in line with the Department's IT Security policy and the Appropriate Use of Portable Digital Storage Devices and Removable Media in Schools policy (This policy is currently in draft format and cannot be accessed until it has been approved. A link to this policy will be made when this policy is released) because the storage is:

- not secure
- not protected against unauthorised duplication, deletion or modification.

4.9.2 External Hard Drives, Flash Cards and USB Drives may be used to temporarily store sensitive information provided they have been protected by approved encryption software. For more information please contact Manager, ICT Services Education.

5.0 PED (Portable Electronic Device) storage includes but is not limited to: Laptops, Personal Digital Assistants (PDAs) and Smart Phones

5.1 As a general rule, no sensitive information is to be stored on PED's, unless encrypted, in line with the Department's IT Security policy and the Appropriate Use of Portable Digital Storage Devices and Removable Media in Schools policy (This policy is currently in draft format and cannot be accessed until it has been approved. A link to this policy will be made when this policy is released) because the storage is:

- not secure
- not protected against unauthorised duplication, deletion or modification.

5.2 Laptops may be used to temporarily store sensitive information provided the laptop has been protected by approved encryption software. For more information please contact Manager, ICT Services Education.

6.0 Disposal of sensitive information

6.1 Disposal of IT storage media must be done in accordance with the Department's IT Security policy. For more information please refer to the following fact sheets available on "index":

- Cleansing/Sanitation of media
- Disposal of Media

6.2 Any unwanted copies e.g. not original file copies of sensitive information, must be shredded or placed in a classified waste bin. Staff should not dispose of any departmental records. All disposal of sensitive information must be done in accordance with the Department's Records Management Program. For further information please contact the Records Management Section.

Attachment:

Attachment A: Sensitive Information Register

Policy Owner: Director, Governance, Regulation and Risk

Related Policies:

DET Records Management Program
Student Recordkeeping Policy
Access to Student Records Policy
DET Information Technology Security Policy
DET Privacy Statement
ACT Protective Security Manual Section 4 Information Security
ACT Government Cabinet Handbook September 2005
ACT Government Security Policy and Guidelines
School Legal Information Manual (SLIM) Module: Privacy