



Department of  
**Education**

[www.deni.gov.uk](http://www.deni.gov.uk)

---

AN ROINN

**Oideachais**

---

MÄNNYSTRIE O

**Lear**

# DE DATA SECURITY POLICY

March 2010

Reviewed and Revised May 2011(DE1/11/56473)

# CONTENTS

## **1**

### **Introduction**

Page 1

## **2**

### **Policy Statement** Page 3

## **3**

### **Accountability and Governance**

Page 4

## **4**

### **Controls, Monitoring and Reporting**

Page 8

## **5**

### **Supporting Legislation / Legislative Context**

Page 11

## **6**

### **Training & Communications**

Page 13

## **7**

### **Information Security Policies and Guidance**

Page 15

# Introduction

# 1

1. Effective data security is a key priority for the Department of Education (DE). It is vital for public confidence and for the efficient, effective and safe conduct of the Department's business. In carrying out its duties effectively DE obtains, processes and manages a broad range of information from the education sector and the citizen. Some of the services provided by the Department directly involve the collection and handling of personal or sensitive data and information which must be managed appropriately and securely.
2. The Department recognises that stringent principles of data security must be applied to all information it holds. This includes sensitive information and personal data on employees, suppliers, contractors and citizens.
3. The Department is committed to ensuring that all the sensitive information entrusted to DE is managed lawfully and appropriately. Legislation including [The Official Secrets Act](#), [The Data Protection Act 1998](#), [Freedom of Information Act 2000](#), [Computer Misuse Act 1990](#) and [The Human Rights Act 1998](#) set the legal framework within which the Department must operate and ensure the safe storage and handling of information. The Department fully appreciates and will take the necessary actions to ensure that it continues to comply with all legislation regarding its management of personal data and other information.
4. While the gathering and analysing of information is essential to the provision of effective public services and the development of relevant and meaningful Government policies, it is clear, nonetheless, that this must be

done in a way that ensures the security of that information and preserves the individual's right to privacy. As a Government department, DE fully accepts that it is its responsibility to safely manage the information with which it is entrusted and to this end DE has in place a range of data security policies and corporate governance and accountability structures to deliver and maintain effective data security.

5. The Department fully accepts the need for transparent accountability and explicit assurance that we will continue to maintain high standards of data security. This responsibility is not limited to the core Department but equally applies to its non-Departmental Public Bodies, delivery partners, contractors, suppliers and any other third party organisation/person established to support the Department in its delivery of services to the public. Therefore, the Department ensures that effective corporate governance arrangements are in place to continually manage and assure all aspects of its approach to data security.
  
6. The specific purpose of this document is to bring together into a single source an overview of the various policies, procedures and structures that have been put in place to ensure the delivery of a safe environment for the handling of the information and data required by the Department to carry out its responsibilities. The data security policies and procedures, in place within the Department, may be found on the "[Security Matters](#)" section of the Intranet. In particular this document sets out:
  - a. The accountability and governance arrangements which are in place to monitor and control performance and give assurance that information is being handled securely,
  - b. The controls and monitoring practices and processes that mitigate against data loss, and
  - c. The various data handling procedures and policies that are in place within the Department.

# Policy Statement

## 2

1. The Department regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between the Department and those with whom it transacts business and the public in general.
2. The Department fully endorses and adheres to the [eight principles of Data Protection](#) as laid out in the [Data Protection Act 1998](#). In particular principle seven, which deals with security states:

***“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”***

3. The Department seeks to foster a culture that values, protects and uses information for the public good through a range of methods and arrangements.
4. The Department works closely with NICS Departments and the [Information Commissioner's Office](#) to ensure compliance with the legal and regulatory framework. The Department will maintain open communication with them about the personal information it holds, how it is used, and citizens' rights with respect to the use of their information.

# Accountability and Governance

## 3

1. Effective accountability and governance arrangements are essential to ensure the proper management and control of information. The following paragraphs detail the various oversight roles and responsibilities that DE has in place to deliver an effective governance regime.

### **Departmental Board**

2. The Departmental Board considers issues which affect the corporate governance of the Department and its NDPBs.

These include:

- progress against performance targets for DE and NDPBs
- finance issues;
- issues relating to audit and accountability; and
- an overview of major policy issues.

The Board is assisted by the Departmental Audit and Risk Management Committee in the oversight and carrying out of its responsibilities.

### **Accounting Officer**

3. The Accounting Officer has ultimate responsibility for data security within the Department and is required to provide, in the annual Statement of Internal Control, assurances that information risks are being controlled and managed and that the Department continues to be a trusted custodian of personal and sensitive information.

### **Departmental Audit and Risk Management Committee**

4. The Departmental Audit and Risk Management Committee assist the Departmental Board in fulfilling its corporate governance responsibilities and oversee the corporate governance and risk management processes. Corporate governance includes internal control relating to operational and compliance controls and risk management which in this context includes data security.

### **Senior Information Risk Owner (SIRO)**

5. The SIRO reports to the Departmental Board on data security matters within the Department, provides assurances that standards are being maintained and reports any incidents that have been identified. This officer is also the Departmental Security Officer (DSO) and as such has broader responsibilities regarding the physical security of the Department.

### **Assistant Departmental Security Officer**

6. The Assistant Departmental Security Officer (ADSO) is based in the Business Support Team of the Equality and All Ireland Directorate in DE and has day to day responsibility for physical security matters. The ADSO supports the DSO on security matters.

### **Information Asset Owner (IAO)**

7. Team Leaders in DE are the IAOs for their individual business areas and are responsible for the secure management of information within their Team(s). They are also the primary liaison contact point for the SIRO on data security matters, including performance reporting; incident reporting; raising information security awareness and audit & accountability matters. In particular it is the responsibility of Information Asset Owners to ensure that:

- They identify the information and assets in their Team and advise the DE SIRO what these are;
- They identify the physical security arrangements for protectively marked/personal/sensitive data, in their Team and advise the DE SIRO if appropriate, secure arrangements are in place;
- Personal/sensitive/other data, in their Team, carries the correct protective marking;
- Where appropriate, data security related risks are included on Directorate Risk Registers, detailing how these risks are managed and mitigated. The DE SIRO should be made aware of any significant data security risks within Teams/Directorates;
- No information carrying a protective marking higher than RESTRICTED is held in TRIM;
- Information carrying a higher than RESTRICTED protective marking is held in the appropriate secure filing cabinet in hard copy;
- Team Disposal Schedules are up to date, reviewed annually and include details regarding the method of disposal for the various types of information recorded.

### **Departmental Information Manager (DIM) and Local Information Managers (LIMS)**

8. The Departmental Information Manager has overall responsibility for the records of the Department and compliance with statutory requirements in relation to information and records management.

Local Information Managers are responsible for information management within their business area. The LIMs help ensure that all information and records management policies are fully implemented and are responsible for compliance by all within their business area.

### **Staff Responsibilities**

9. The role played by individual staff members is vital in ensuring information is held securely. To that end all staff must take responsibility for the protection of protectively marked/personal/sensitive information that they manage or

access as part of their day to day work activities. It is therefore essential that all DE staff are familiar with the Department's data security policies. Staff must ensure that all protectively marked/personal or sensitive information in their possession is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular it is the responsibility of staff to ensure that:

- paper files and other records or documents containing protectively marked/personal/sensitive information are kept in a secure physical environment;
- protectively marked/personal/sensitive information held on computers and computer systems is stored in line with the IT security policies;
- if they are required to pass information to an organisation outside the Department, that they follow the guidance as set out in OFMDFM's ["Guide to Document and IT Security"](#).
- protectively marked/personal/sensitive data is correctly secured if transmission of this type of data is necessary;
- protectively marked/personal/sensitive data is correctly disposed of, in line with Team Disposal Schedules.

10. In addition to their responsibilities as members of staff, line managers have a responsibility to ensure there are appropriate procedures in place so that the required authorisations are secured before any personal/sensitive information is released outside the business area.

11. Attached at [Annex A](#) is a chart describing the data security governance and reporting structure in the Department.

# Controls, Monitoring and Reporting

## 4

1. Effective controls, monitoring and reporting procedures are necessary to ensure that high data security standards are in place and are being maintained. To that end the following range of measures are in place to provide assurance that data security and business risks within the Department are properly managed.

### **Statement of Internal Control**

2. The Statement of Internal Control (SIC) is an annual statement made by the Accounting Officer as part of the Department's Resource Accounts. In it the Accounting Officer comments on a range of risk and control issues. To adequately make his statement the Accounting Officer needs comprehensive and reliable assurance from managers, internal audit and other assurance providers that risks, including information risks are being managed effectively. From 2008/09 the SIC includes a specific reference to the handling of information risk issue within the Department.

### **Annual Security Report**

3. The Security Advisory Unit in OFMDFM provides the Head of the Northern Ireland Civil Service with an annual report on the efficiency and effectiveness of the protective security arrangements across NI Departments. DE provides information for this report.

### **Risk Register**

5. The assessment and management of risk is central to good corporate governance. This is no less true for the management and securing of information. Therefore each Team Risk Register must include a specific

information risk and detail how the risk is managed and mitigated. Risk registers are reviewed quarterly and reported to the Departmental Board as part of the risk management system.

### **Incident Monitoring and Reporting**

6. An important aspect of the Department's information security policies is the effective and timely reporting of all suspected incidents of misuse or loss of protectively marked/ personal/sensitive information or breaches of data security. The Department has in place guidance "[Reporting the misuse/loss of protectively marked/personal/sensitive data](#)" on the "Security Matters" Intranet site, outlining steps which must be followed when reporting such incidents.
7. It is the responsibility of the Departmental Security Officer to oversee, in consultation with OFMDFM's Security Advisory Unit, investigations into suspected data misuse/loss incidents and where necessary:
  - inform the Information Commissioner's Office of the suspected incident;
  - activate a response plan to the incident, and
  - report to the Departmental Board if appropriate

### **Delivery Partners, Consultants, Contractors and Suppliers**

8. The Department will from time to time enter into arrangements with a range of other organisations to support it in delivering its services. These may include organisations in the private, community and voluntary sectors. Such organisations will often be contracted to undertake services or work which will require them having access to, handling, storing or disposing of information.
9. It is essential that in entering into contractual arrangements with such organisations sponsoring Teams ensure that the Department's information security standards are maintained and protected.

10. Therefore, it is the responsibility of each individual sponsoring Team to ensure that when entering into a contract with an outside organisation:

- Data security is accurately reflected in the contract;
- the contracted organisation is fully aware of the Department's Data Security Policy
- Data Security will be a standing item on all formal monitoring and reporting mechanisms
- The contracted organisation must sign a declaration confirming that they have read, understand and agree to abide by DE's Data Security Policy.

11. To assist in the delivery of effective and robust contracts the Department commits to using the Central Procurement Directorate (CPD) for such procurements and the Department will continue to work with CPD to ensure data security matters are accurately reflected in these contracts.

# Supporting Legislation / Legislative Context

## 5

1. There are three main pieces of legislation currently in force that require the Department to disclose information. Detailed guidance on these can be accessed via the following links –  
[Freedom of Information Act 2000](#);  
[Environmental Information Regulations 2004](#);  
[Data Protection Act 1998](#).

3. In particular the Data Protection Act 1998 (DPA) regulates the processing of 'personal data' (defined as any information about an identifiable living individual) by requiring all organisations that handle personal information to comply with a number of important principles regarding privacy and disclosure. The essential features of the DPA are that it:

- a. requires organisations holding personal data to notify the Information Commissioner in broad terms of what they hold, and for what purpose(s);
- b. requires organisations holding personal data to comply with eight data protection principles, and
- c. provides for individuals to be told, on request, what data is held about them (subject-access) and gives them rights to correct any errors, prevent processing, etc.

4. In relation to information security, the seventh data protection principle states that,

***"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."***

## **Handling Requests for Information**

5. As well as having a duty to protect the information we hold, we are also required by the Freedom of Information Act and the Data Protection Act to make information available to the public on request. In responding to requests from the public, we must ensure that sensitive information is not accidentally or inappropriately released, while at the same time meeting the Department's obligations to disclose. It is therefore important that all staff are made aware of the statutory framework within which we are required to disclose information, such as subject access requests (DPA) and other types of requests (FOI); are able to recognise requests to which these requirements apply; and are familiar with handling such requests.
  
6. Advice and practical support on the handling of individual requests is also available by contacting the Information Management Section of the Business Support Team. DE's FOI Procedures Manual (TRIM Ref: DE1/11/21274) was revised and issued to all staff in March 2011. DE's Policy and Guidelines for staff on Data Protection was also revised in April 2011 – Policy (TRIM Ref: DE1/11/27177) Guidelines (TRIM Ref: DE1/11/27178).

# Training and Communications

## 6

1. The Department recognises that effective training and good communications are essential if a secure data environment is to be maintained. Therefore, a range of approaches are used to ensure that all staff have the necessary knowledge, awareness and skills to ensure that the Department delivers a safe environment for the management of the information it holds.

### **NICS Wide Training**

2. DE will ensure that all centrally mandated information security training is fully implemented within the Department.

### **Departmental Induction**

3. It is important that all new staff joining DE are made aware of the Department's data security policy and related procedures and guidelines. To this end the staff induction process within Teams contains a section on data security which emphasises the importance attached to information management in the public sector in general, DE and in particular their own business area. The effective induction of new staff relies on the training processes within Teams. Therefore, it is incumbent on all line managers to ensure their new staff are familiar with this policy, DE's [Clear Desk Policy](#) and all local Team specific guidance and procedures. The Departmental Intranet has a specific section on "Security Matters", which contains a range of advice, guidance and policies on security related issues and is also used to disseminate Departmental data security policies to both new and existing staff.

### **Records Management training**

4. Effective management of records can ensure information is handled correctly. Training is available on Records Management, through the Centre for Applied Learning (CAL) and the Information Management Section of the Business Support Team will provide advice and guidance on specific issues.

### **Communicating the Data Security message**

6. The Department is committed to maintaining an appropriate profile on data security matters and will use internal communications activities to ensure the message is delivered to all staff.

# Information Security Policies and Guidance

## 7

1. The following is a list of current information security related policies in force within the Department with links attached. If a secure and effective information environment is to be maintained within the Department it is essential that staff should be familiar with and fully apply the policies and advice set out in these documents.

[A Guide to Document and IT Security](#)

2. This guide, published by OFMDFM, is intended to provide a ready reference on matters relating to document and IT security. The standards and procedures in the guide are the minimum which must be applied uniformly throughout all Departments and Agencies.

3. [10 Key Rules on Securing Sensitive Data](#)

This document sets the 10 key rules that all NICS staff must follow to ensure the security of personal data.

4. Annex 9 of Section 6.01 “Standards of Conduct”, of the NICS Handbook, which is available to all staff via the HRConnect Portal, sets out the policy of the Northern Ireland Civil Service (NICS) in relation to the use of Internet and e-mail facilities on departmental or agency Information and Communications Technology (ICT) resources. The policy applies to all NICS staff and others given permission to use departmental or agency resources to access Internet or email facilities. DE Guidance on the Use and Management of Email has been updated – see document DE1/11/55997.

### [DE Security Operating Procedures](#)

5. This document sets out mandatory guidance for DE staff in the use of IT facilities and includes guidance on passwords, access to IT resources and Internet and email use.

### [IT Assist Asset Disposal Procedures](#)

6. DE IT hardware and software are now IT Assist assets and must be disposed of according to the guidance above.

### [DE Anti Fraud Policy & Fraud Management](#)

7. The Department's Fraud Policy covers any fraudulent use of information – personal, sensitive or classified which is held by the Department

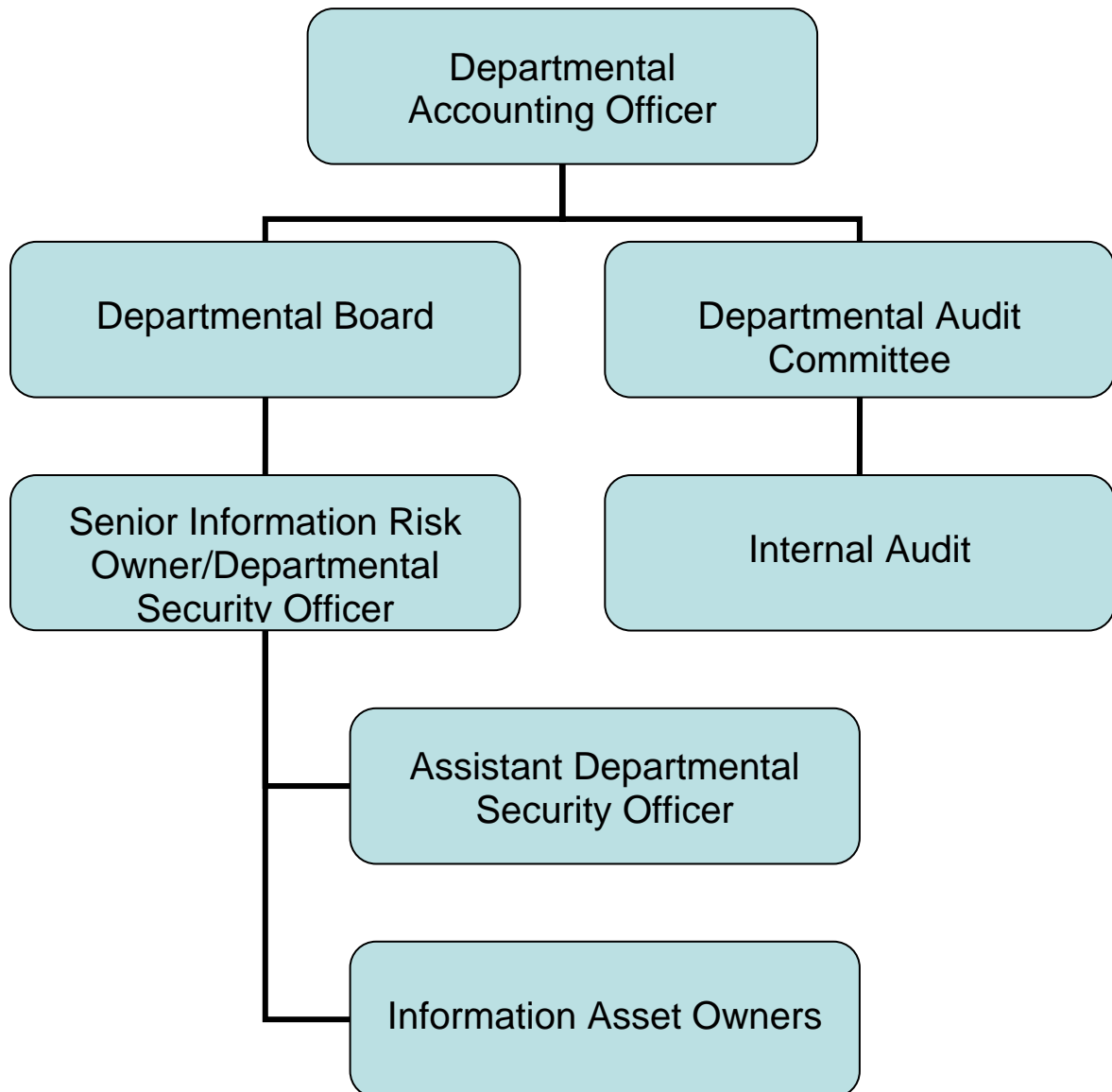
### [Central Procurement Directorate](#)

8. The Department has a Service Level Agreement with the Central Procurement Directorate (CPD) in DFP to use its services for tendering and procuring goods and services. CPD must be used for all procurement exercises for services which will include the handling, use, storage or transmission of information.
9. Central Procurement Directorate have in place a set of information security related clauses in its standard Terms & Conditions, used for all contracts tendered for through them. It is the responsibility of the commissioning officer within DE to ensure that these clauses are sufficient for the services they are planning to procure. If additional safeguards are required as part of the contract the commissioning officer should speak with the DE Account Manager in CPD. The Department has the right to include additional safeguards, in the tender documentation that issues, as part of the tendering process for the service being sought.
10. In addition to the specific policies and guidance documents listed above the Cabinet Office have issued [Her Majesty's Government \(HMG\) Security Policy Framework](#). While this framework does not formally apply to the

Northern Ireland Civil Service it has been agreed that NI Departments should adopt its policy and procedures as best practice.

## Annex A

### Data Security Governance and Reporting Structure



**WENDY REID**  
**Assistant Departmental Security Officer**  
**Business Support Team**  
**Ext 59845**