Department of
Education
www.education-ni.gov.uk

DE DATA SECURITY POLICY

Document Version History

Content Manager (CM) Ref.	Date	Comments
DE1/10/28819	March 2010	First issued to DE staff
DE1/11/56473	May 2011	Reviewed & Reissued
DE1/13/43745	May 2013	Reviewed & Reissued
DE1/13/43745[v2]	January 2015	Reviewed & Updated for new intranet website
ED1/16/32615	17 June 2016	1st review, to include revised guidance on reporting data security breaches
ED1/16/56408	27 July 2016	2nd review (DSO)
ED/1/16/56408	23 February 2017	Web links updated
ED1/18/74349	10 April 2018	Full document review + incorporation of EU GDPR and Data Protection Act 2018
ED1/20/238717	17 September 2020	Full document review and update
ED1/20/238717	11 February 2021	Document updated for Content Manager
ED1/20/238717	25 February 2022	Document reviewed. Links updated.
ED1/20/238717	27 November 2025	Document Reviewed + incorporation of A.I. considerations
ED1/20/238717	14 May 2026	Document updated to include the Data (Use and Access) Act 2025
ED1/20/238717	May 2027	Due for Review

CONTENTS

1 Introduction

1.1 Effective data security is a key priority for the Department of Education (DE). It is vital for public confidence, ensuring the efficient, effective and safe conduct of the Department's business. In carrying out its duties effectively DE receives, processes and manages a broad range of information from the education sector and the public. Some of the services provided by DE directly involve the collection and handling of Personal or Special Category (Sensitive) Personal data which must be managed appropriately and securely.

1.2 DE recognises that stringent principles of data security must be applied to all information it holds. This includes Personal and Special Category data on employees, suppliers, contractors and citizens, as well as business sensitive information.

1.3 DE is committed to ensuring that all Personal and Sensitive Personal information entrusted to DE is managed lawfully and appropriately in compliance with information legislation.

The UK General Data Protection Regulation (UK GDPR) 2018; the Data Protection Act 2018; the Freedom of Information Act 2000; the Environmental Information Regulations 2004; the Public Records Act 1923; the Computer Misuse Act 1990; the Human Rights Act 1998; and the Official Secrets Act 1989 set the legal framework within which DE operates, ensuring the secure storage and handling of information. The Department is committed to maintaining full compliance with all relevant legislation governing the management of personal data and sensitive information. In addition, the Data (Use and Access) Act 2025, which updates the UK GDPR, the Data Protection Act 2018, and e-privacy regulations to facilitate responsible innovation while upholding robust privacy protections, will be integrated into all Departmental data handling policies and practices.

1.4 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 rights and freedoms. DE fully accepts that it has responsibility to safely manage the information with which it is entrusted and to this end has put in place a range of data security policies and corporate governance and accountability structures to deliver and maintain effective data security.

1.5 DE acknowledges 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 Arm's Length Bodies, delivery partners, contractors, suppliers and any other third party organisation/person established to support the Department in its delivery of services. Therefore, the Department will endeavour to ensure that effective corporate governance arrangements are in place to continually manage and assure all aspects of its approach to data security.

The specific purpose of this document is to provide 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 DE to carry out its responsibilities. The data security policies and procedures, in place within DE, may be found on the Intranet site via Topics - Information Management – Information Assurance. 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 in DE.

2. Policy Statement

2.1 The Department regards the lawful and correct handling of personal data 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.

2.2 In undertaking its official functions the Department processes personal data in line with the requirements of the UK GDPR and its six principles: Guide to the UK General Data Protection Regulation (UK GDPR)

2.3 DE seeks to foster a culture that values, protects and uses information for the public good through a range of methods and arrangements.

2.4 DE works closely with NICS Departments and the Information Commissioner's Office (ICO) to ensure compliance with the legal and regulatory framework. The Department will maintain open communication with them about the personal data it holds, how it is used, and citizens' rights with respect to the use of their information.

3. 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.

3.2 **Departmental Board (DB)**

The DB considers issues which affect the corporate governance of the Department and its Arm's Length Bodies (ALBs). These include:

- progress against performance targets for DE and ALBs;
- 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 Assurance Committee (ARAC) in the oversight and carrying out of its responsibilities.

3.3 **Permanent Secretary - Accounting Officer (AO)**

The AO has ultimate responsibility for Data Security within DE and is required to provide, in the annual Departmental Security Health Check (DSHC) Report and the Statement of Internal Control, assurances that information risks are being controlled and managed and that DE continues to be a trusted custodian of personal and Special Category personal information.

3.4 **Departmental Audit and Risk Assurance Committee (ARAC)**

ARAC assists the DB 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.

3.5 **Senior Information Risk Owner (SIRO) – Director of Corporate Services and Governance**

The SIRO reports to the DB on data security matters within DE, provides assurances that standards are being maintained and reports any incidents that have been identified. The SIRO advises the AO on the information risk aspects of the Statement of Internal Control.

3.6 **Data Protection Officer – (DPO) -** Team leader Information Management Team (IMT)

The DPO is a dedicated and key supporting role that underpins the Accounting Officer function carried out by the Permanent Secretary. The DPO is the cornerstone of accountability for Data Protection in DE and provides full authoritative advice in this area. The DPO also heads up IMT.

3.7 **Departmental Security Officer (DSO) –** Team Leader Departmental Business Services Team (DBST) – Corporate Services and Governance Directorate (CSGD)

The DSO has day to day responsibility for all aspects of Protective Security including Physical, Personnel and Information Security. The post holder also has responsibility for the implementation and dissemination of protective security

policy, personnel security matters, incident reporting and information assurance training.

3.8 **Assistant Departmental Security Officer (ADSO)** – Deputy Team Leader DBST – CSGD

The ADSO has day to day responsibility for Personnel and Physical Security matters. They provide a range of advice and guidance to departmental staff as required and ensure good practice. They attend and represent DE's interests at the Interdepartmental Security Officers Forum (ISOF). The ADSO supports the DSO and SIRO on security matters.

3.9 **Information Asset Owner (IAO)**

All Team Leaders (Grade 7s) 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 accountable to the SIRO on Data Security matters, including performance reporting; incident reporting; raising information security awareness and audit & accountability. In particular it is the responsibility of IAOs to ensure that:

- They identify all information and assets held by their Team and ensure that these are recorded in their business area Information Asset Register (IAR);
- They identify the physical security arrangements for protectively marked/Personal/Personal Sensitive data, held by their Team;
- 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 OFFICIAL-SENSITIVE is held in Content Manager (CM), formerly HPRM/TRIM;
- Information carrying a higher than OFFICIAL-SENSITIVE protective marking, i.e., Secret or Top Secret, is held in the appropriate security furniture in hard copy;
- They review their relevant business section within the approved DE Records Retention and Disposal Schedule, and provide details regarding the method

of disposal for any types of new information created, which is not already covered in the existing DE schedule and notify same to the Information Management Team, who will include in a corporate review of the schedule which is resubmitted to PRONI/Assembly for renewal, normally in around 3 year cycles.

- They provide an annual Assurance Statement which forms part of DE's response to the Departmental Security Health Check (DSHC) exercise.

3.10 **IT Security Officer (ITSO) - Departmental Business Services Team (DBST) – Corporate Services and Governance Directorate** – local DE post covered by IT Assist.

The ITSO has day to day responsibility for IT security matters. The ITSO provides advice and guidance to DE staff and their education partners on information assurance and acts as Incident Response Handler in the event of a major incident affecting information systems in the department. They attend and represent DE's interests at the ITSO forum and ensure good practice. The ITSO reports to the DSO on IT security matters.

3.11 **Departmental Accreditor - Departmental Business Services Team (DBST) – Corporate Services and Governance Directorate**

The Accreditor is responsible for the accreditation of Line of Business systems that operate in the department and oversee the accreditation process. They represent DE on the NICS Risk and Information Assurance Council (RIAC).

3.12 **Departmental Information Manager (DIM)**

Based in IMT, the DIM has departmental responsibility for the records of the Department and compliance with statutory requirements in relation to information access and records management.

3.13 **Local Information Managers (LIMs)**

LIMs are responsible for routine information management issues within their business area and help to ensure that all information and records management

policies are fully implemented and ensuring compliance by all within their business area.

3.14 **Individual Staff Responsibilities**

Every individual staff member has a vital role in ensuring information is held securely. To that end all staff must take responsibility for the protection of protectively marked/Personal/Sensitive Personal information that they manage or handle as part of their day to day work activities and ensure that they do so in compliance with relevant legislation and in line with DE/NICS policies and procedures, which are based on best practice standards.

3.15 It is therefore essential that all DE staff are familiar with this policy and other related Data Security guidance linked to this document. Staff should ensure that all protectively marked/personal or sensitive personal 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 Personal information are kept in a secure physical environment;
- protectively marked/personal/sensitive personal information held on computers and computer systems such as CM) 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 the “NICS Guide to Physical, Document and IT Security"
- protectively marked/personal/sensitive personal data is correctly disposed of, in line with the DE approved Records and Disposal Schedule.

3.16 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 Personal information is released outside the business area.

Annex A is a chart describing the DE Data Security governance and reporting structure.

4 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 DE are properly managed.

Statement of Internal Control

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

Departmental Security Health Check (DSHC)

4.3 The Central Information Assurance Team in the Department of Finance (DoF) are responsible for the production of the annual NICS Security Report for the Head of the Civil Service. This is an assessment of each Department's management of Security and information risk. The report also requires DE to seek information assurances from their ALBs and to comment on their Data Security arrangements with their delivery partners and third party suppliers.

Risk Register

4.4 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 Directorate Risk Register and the DE Corporate Risk Register identify Data Security related risks and detail how these risks are 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

4.5 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 personal information or breaches of Data Security. The DE Personal Data Breach Policy Management Plan provides guidance on reporting the misuse/loss of protectively marked/personal/special category data, in line with the UK GDPR:

General Data Protection Regulation 2016 and Data Protection Act 2018 (GDPR/DPA)

4.6 It is the responsibility of the DSO to oversee, in consultation with The Executive Office's (TEO's) Security Advisory Unit, as required, investigations into suspected data misuse/loss incidents and where necessary:

- consult with the DE DPO;
- inform the ICO of the suspected incident;
- activate a response plan to the incident, and
- report to the DB if appropriate

Delivery Partners, Consultants, Contractors and Suppliers

4.7 DE 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 Departmental related information. Officials entering into contracts or alternative arrangements such as MOUs or Data Sharing Agreements for DE, must ensure that they comply with DE guidance and the requirements of the UK GDPR.

4.8 Third party organisations may represent an area of risk and therefore DE must ensure that appropriate security controls are in place to reduce risk to an acceptable level, along with effective governance controls to monitor compliance and respond to incidents. It is essential that in entering into contractual

arrangements with such organisations sponsoring Teams ensure that DE's information security standards are maintained and protected.

4.9 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 is 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;
- The Delivery Partner should, when requested, provide their sponsor Team with the appropriate Information Assurance on DE related information that they have access to, are handling, transmitting, storing or disposing of as part of their work for the Department;
- The Delivery Partner should complete an annual Assurance Statement for the sponsor Team, when requested, as part of the annual DSHC exercise.

4.10 To assist in the delivery of effective and robust contracts DE uses DoF's Construction and Procurement Delivery (CPD) for such procurements and DE will works with CPD to ensure data security matters are accurately reflected in these contracts.

5. Supporting Legislation/Legislative Context

5.1 There are a number of pieces of legislation currently in place that govern the disclosure of departmental information. These can be accessed via the following links –

Freedom of Information Act 2000;

Environmental Information Regulations 2004;

UK General Data Protection Regulation 2018

Data Protection Act 2018

5.2 UK data protection legislation regulates the processing of 'Personal Data' (defined as any information about an identifiable living individual) by requiring all organisations that handle personal data to comply with a number of principles regarding privacy and disclosure and to ensure that the rights of data subjects are observed:

Article 5 Principles relating to processing of personal data

5.3 **Handling Requests for Information**

Together with having a duty to protect the information DE holds, the Department is also required by the FOI Act and the UK data protection legislation to make information available to the public on request. In responding to requests from the public, we must ensure that only appropriate data/information is released in compliance with the relevant legislation, while at the same time meeting the Department's obligations to disclose information when it is legally appropriate to do so. It is therefore important that all staff are aware of the statutory framework within which we are required to disclose information under the UK data protection legislation, such as Subject Access Requests (SARs) and other types of information requests under the FOIA and are able to recognise requests under the relevant legislation and are familiar with handling such requests.

5.4 Advice and guidance on the handling of requests for information is available on DE's Intranet site and from IMT.

6 Training and Communications

6.1 DE 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 DE delivers a safe environment for the management of the information it holds.

NICS Training

6.2 IMT will promote the full implementation of centrally mandated information security training within the Department. However, line mangers and IAOs have a responsibility to ensure their staff complete mandatory training too.

Departmental Induction

6.3 It is important that all new staff joining DE are made aware of DE'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, that they implement the NICS Clear Desk Policy and all local Team specific guidance and procedures. DE's Intranet contains a wide range of advice, guidance and policies on security related issues and is also used to disseminate DE's Data Security & Information Management and Assurance policies to both new and existing staff.

Records management training

6.4 The effective management of records can ensure information is handled correctly. IMT can advise new staff joining DE of what training in the use of CM is available and appropriate.

Communicating the Data Security message

6.5 DE 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.

7 Information Security Policies and Guidance

7.1 A suite of advice, guidance and policies is available to staff on the IMT area of the DE Intranet. If a secure and effective secure information environment is to be maintained within the Department, it is essential that all staff should be familiar with and fully apply the policies and advice set out in these documents:
Information Security Policies and Guidance

7.2 The NICS Handbook section 6.11- Use of Electronic Communications, 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.

7.3 In addition to the specific policies and guidance documents listed above the Cabinet Office have issued the Governments Security Policy Framework. NI Departments have adopted this document as best practice:
HMG Security Policy

8 Use of Generative Artificial Intelligence (AI)

8.1 DE recognises the growing role of Generative AI technologies in supporting departmental business and educational outcomes. The adoption and use of AI must be carefully managed to ensure compliance with data protection legislation.

8.2 The integration and use of these emerging technologies are subject to continual review and must be approached with caution taking into account the data protection and information security risks.

8.3 Staff are reminded that the use of these technologies should be limited to approved platforms and must remain within the confines of the Departmental and wider NICs policies.

8.4 Where AI tools are used to process personal or sensitive information, appropriate assessments and arrangements should be considered and advice should be sought from the Data Protection Officer.

8.5 Staff are expected to remain aware of their responsibilities under departmental and NICS policies on use of these technologies.

Annex A

Data Security Governance and Reporting Structure