Department of Education and Skills

Protection of Personal Data

Code of Practice

AN ROINN OIDEACHAIS AGUS SCILEANNA | DEPARTMENT OF EDUCATION AND SKILLS

Records Management Unit **February 2011**

Table of Contents

Foreword 2
Introduction from the Data Protection Commissioner 3
Introduction from the Secretary General 3

What is personal data? 4
What type of personal data do the Acts apply to? 4
What is 'identifiable' information? 4
What is sensitive data? 4

What does this mean for individuals? 5

What does this mean for the Department? 6
Registration with the Data Protection Commissioner 6

Data Protection Rules 8

Responsibility of Employees 14

Audits of Procedures 14

Role of the Data Protection Commissioner 15

Protocol for reporting breaches 16

APPENDIX 1 Definitions 17
APPENDIX 2 Enforcement of Data Protection Legislation 18
APPENDIX 3 Applying for Access to Personal Data 19

Foreword

This Code of Practice sets out the requirements of the Data Protection Acts, the steps to be taken by the Department of Education and Skills when processing personal data and how the Department will respond to requests for access to personal data. This Code of Practice will be updated, as required, to include any changes to the type of data collected and processed by the Department.

All Department staff **must** comply with the provisions of the Data Protection Acts 1988 and 2003 when collecting, handling and storing personal data. This applies to personal data relating to both employees of the Department and individuals who interact with the Department, e.g., teachers, students, parents/guardians, etc.

This Code of Practice applies to all staff of the Department of Education and Skills, both permanent and temporary staff, to staff working on a contract basis for the Department and others who are authorised to access personal data held by the Department. Staff should familiarise themselves with Data Protection issues by reading this Code of Practice and the following related documents which are all available on the Department's Intranet or from the Records Management Unit:

- Data Protection Guidelines
- Data Protection Breach Policy
- Policy for the Protection of Data while using Laptops and other Mobile Data Devices

Line managers within the Department are required to ensure that all staff who handle or have access to personal data comply with this Code of Practice. Principal Officers in the Department are required to review procedures in their areas to ensure compliance with this Code of Practice as part of the annual Business Planning process.

Introduction from the Data Protection Commissioner

I am very happy to be able to formally approve this Code of Practice under the terms of Section 13 of the Data Protection Acts 1988 and 2003. The Code is the result of intensive work by the Department of Education and Skills and its staff, working in close co-operation with my Office. It is designed to give operational meaning to the principles of data protection set out in European and National law.

I am confident that the Code will make a significant contribution to improving knowledge and understanding of data protection within the Department of Education and Skills. I intend to continue to work closely with the Department of Education and Skills and its staff to ensure that the guidance set out in the Code is followed in daily practice.

Billy Hawkes
Data Protection Commissioner

Introduction from the Secretary General

Data (including information and knowledge) is essential to the administrative business of the Department. In collecting personal data the Department has a responsibility to use it both effectively and ethically. There is a balance to be struck between an individual's right to privacy and the legitimate business requirements of the Department. Therefore, it is critical that all staff in the Department work to the highest attainable standards. Our integrity includes both the way in which we conduct ourselves and the way in which we ensure the data we hold is compliant with relevant legislation.

Set against the Data Protection Acts 1988 and 2003, the aim of this Code of Practice is to ensure each employee of the Department has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This, in turn, will assist the Department in its compliance with the Acts.

Protecting our data is common sense. We need to ensure that data gathered and processed by the Department is compliant with Data Protection Legislation. The reading and understanding of this Code of Practice by all employees will go a long way towards meeting this requirement.

Further advice in relation to the storage, handling and protection of personal data is available in the Department of Finance Guidelines, "Guidance Note on Protecting the Confidentiality of Personal Data"

Brigid McManus
Secretary General

What is personal data?

Section 1 of the Data Protection Act provides the following definition of personal data:

> "Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."

Data for the purpose of safeguarding the security of the State and data required by law to be made public are excluded from the provisions of the Acts. However, if that data is then used for another purpose, provisions of the Acts apply.

What type of personal data do the Acts apply to?

The provisions of the Acts apply to any personal data that is processed by the Department. It does not matter how the personal data is stored – on paper, on an IT system, on laptops, mobile data devices, CCTV etc.

Employment records and related information such as absence/attendance records, injury or sickness details, disciplinary or performance records, interview results etc., are all covered by the Acts as are all personal data about employees kept on computer or word processor disk.

Often a case by case assessment must be made taking account of some of the above considerations as to whether data would be deemed to be personal. Further guidance on the definition of personal data is available on the Data Protection Commissioner's website at www.dataprotection.ie.

What is 'identifiable' information?

There are different ways in which an individual can be considered 'identifiable'. A person's full name is an obvious identifier. A person can also be identifiable from other information, including a combination of information such as physical characteristics, occupation, address, etc.

What is sensitive data?

The definition of sensitive personal data as contained in the Data Protection Acts is as follows:

""sensitive personal data" means personal data as to -

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
(b) whether the data subject is a member of a trade-union,
(c) the physical or mental health or condition or sexual life of the data subject,
(d) the commission or alleged commission of any offence by the data subject, or
(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

and any cognate words shall be construed accordingly."

What does this mean for individuals?

The Data Protection Acts of 1988 and 2003 confer a number of rights, including:

- Every person has the right to **access personal data** held on computer or in a manual filing system. A person can make a subject access request to any organisation or any individual who holds personal data about them (response to be given promptly but in any event no later than 40 days from receipt of the request).

- Every person has a right to be given a **description** of the data about them and the purposes for which it is kept (response to be given within 21 days of request).

- If the data held about an individual is inaccurate they have a right to have that data corrected or annotated. In some cases the person may request that the data is erased – for example if the body keeping the data has no good reason to hold it or if the data has not been obtained fairly. A person can also request that the data be blocked i.e., to prevent it from being used for certain purposes. For example, a person may block their data being used for research purposes where it is held for other purposes.

Any individual who suffers damage through the mishandling of personal data may be entitled to claim compensation through the courts of law.

In particular, Section 7 of the Data Protection Act, 1988 makes it clear that an employer who holds personal data on any employee owes a duty of care to that employee. Any compensation claims are a matter for the courts – the Data Protection Commissioner has no function in the matter.

What does this mean for the Department?

Registration with the Data Protection Commissioner

Under the Data Protection Acts 1988 and 2003, certain categories of data controllers (those who control the contents and use of personal data) and certain categories of data processors (those whose business consists wholly or partly in processing such data for others) must register with the Data Protection Commissioner (DPC). The register of data controllers and processors is a public register intended to bring transparency to the processing of personal data. All register entries are available on the DPC website www.dataprotection.ie

For registration purposes, data held by the Department of Education and Skills has been grouped under a number of different areas. These areas and their purpose for collecting personal data are listed below:

School Staffing and Payroll Services:

- Payroll payment on a fortnightly basis of serving and retired teachers and special needs assistants in primary, voluntary secondary, community and comprehensive schools, a number of serving and retired clerical officers and caretakers in primary and voluntary secondary schools and a number of child-care workers in primary schools

- Personal data on ancillary school staff who are employed in schools where a new building is to be provided via Public Private Partnership

- Personnel and payroll services for Visiting Teachers for Traveller children and children with a visual or hearing impairment

- Administration and regulation of pension matters of education sector staff

- Industrial relations and employment legislation issues

- Secondment of Irish teachers to European schools.

Services to Schools and VECs:

- Assistance to school authorities and VECs by providing policies and supports in relation to their role as employers of teachers and Special Needs Assistants

- Administration of services in respect of schools – including collection of personal data of post primary students in order to provide financial support to schools, to allocate teaching resources to schools and to facilitate policy formulation

- Operation of an inspection and evaluation programme, including school, teacher and subject inspection, programme inspection and Whole School Evaluation.

Special Needs and Social Inclusion Services:

- Assessment of suitability of those nominated by the National Voluntary Childcare Organisations for the role of Síolta co-ordinators

- Provision of a school transport service for students at primary and post primary levels

- Provision of education support services for children with special educational needs

- Provision of educational psychological service to primary and post primary schools

- Provision of personal records to former residents of industrial and reformatory schools, to the Commission to Inquire into Child Abuse and to the Residential Institutions Redress Boards

- Management of the response in cases where litigation has been initiated or threatened against the Minister on behalf of children and adults with special educational needs

- Administration of services in High Support Special Schools, Youth Encounter Projects and Line Projects

- Provision of education support services by the Visiting Teacher Service in respect of Traveller children and Children with a visual or hearing impairment

- Confidential records of child protection and welfare referrals to Health Service Executive (HSE) and internal referrals to the Department of Education and Skills Schools Division.

Further and Higher Education Services:

- Funding and development of student support services to enable students undertake higher and further education programmes

- Some records of staff and former staff of Institutes of Technology are retained by the Department as a requirement of relevant legislation

- WorldSkills Competition

- Identification of teachers claiming payments for Locally Devised Assessments

- International Programmes i.e., Third level expert exchanges organised under cultural arrangements; Post Graduate scholarships application

dossiers and Undergraduate and Post Graduate applications to go as English Language Assistants to schools in Germany, Austria, Italy, France and Spain.

Policy Advice, Development and Review Services:

- Applications for funding for research and development project.

Corporate Services:

- Details in respect of staff of the Department
- Correspondents with the Department's Press Office, Offices of the Minister and Ministers of State, Office of the Secretary General, Regional Office Service and Corporate Services
- Personal data provided by service providers.

An officer at Principal Officer level has been assigned responsibility as a Data Controller for each of the areas above. A compliance checklist is available on the Data Protection Intranet page to help sections in the Department assess their compliance with this Code of Practice.

Data Protection Rules

Staff in the Department, in particular section managers, should ensure that adequate processes and procedures are in place to ensure that the collection, storage and processing of personal data is carried out in a way that is compliant with the provisions of the Data Protection Acts. There are eight rules which should be applied when collecting, storing and processing personal data.

Eight Rules of Data Protection

1. Obtain and process the data fairly
The Department will collect and process (or use) personal data fairly. Forms (either electronic or paper) requesting personal data issued from the Department will state what the data will be used for and who will have access to the data. Secondary or future uses for the data, which might not be obvious to individuals, will be brought to their attention at the time of obtaining personal data. Individuals will be given the option of saying whether or not they wish their data to be used in these other ways. If the Department has data about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the data was collected), individuals will be given an option to indicate

whether or not they wish their data to be used for the new purpose, except in exceptional circumstances where the Department is obliged by law to disclose the data or is permitted by law to use the data in this manner without the consent of the individual. In instances where personal data is exchanged with the Department of Social Protection the exchange will be with the consent of the data subject and/or covered by legislation, including the Social Welfare Consolidation Act 2005.

A detailed listing of all personal data collected by the Department is available on the public register held by the Data Protection Commissioner's Office. http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/default.asp&CatID=27&m=g The Department's registration number is 10764/A.

2. Keep the data only for one or more specified, explicit and lawful purposes

The Department cannot keep data about people unless it is held for a specific, lawful and clearly stated purpose. It is therefore unlawful to collect data about people routinely and indiscriminately, without having a sound, clear and legitimate purpose for so doing.

Personal data obtained and processed in the context of administrative work will state clearly what these data items are; the purpose for collecting it; and that it is obtained and processed in compliance with the Data Protection Acts.

There is a strict statutory basis providing for the use of the Personal Public Services Number (PPSN), which allows the Department to use the PPSN in support of a provision of a public service to a customer. The Department is required to register with the Department of Social Protection stating what the PPSN is used for and any future plans for such use. Details of this registration are available on the Department of Social Protection website at: http://www.dsfa.ie/EN/Topics/PPSN/Pages/rou.aspx

3. Use and disclose only in ways compatible with the purposes for which data were initially given

Personal data obtained for a particular purpose, may not be used for any other purpose and the Department may not divulge the personal data to a third party, except in ways that are "compatible" with the specified purpose. The Department will use and disclose personal data in a way in which those who supplied the data would expect it to be used and disclosed. Staff must follow the procedures set out in the Data Protection Guidelines (on the intranet) when dealing with enquiries for access to personal data.

Transfers of personal data to agents who are carrying out operations upon the data on behalf of the Department and not retaining it for their own purposes, does not constitute "disclosures" of data for the purposes of the Act.

Examples of such transfers would include the transfer of staff data to a separate payroll company for payroll administration purposes. Such data transfers are covered by a contract Data Processing Agreement.

A list of the persons or bodies (or categories of them) to whom personal data collected by the Department is disclosed is shown in the Department's registration with the Data Protection Commissioner's Office http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/default.asp&CatID=27&m=g.

The restriction on processing of personal data (including disclosure to a third party) is lifted in a limited number of circumstances, specified in Section 8 of the Data Protection Acts, as follows:

- Required for the purpose of safeguarding the security of the State
- Required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid
- Required in the interests of protecting the international relations of the State
- Required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property
- Required by or under any enactment or by a rule of law or order of a court
- Required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness.

4. Keep data safe and secure

High standards of physical and technical security are essential to protect the confidentiality of personal data. The standards in place in the Department are:

- For Data Protection purposes, in order to ensure that access to personal data is restricted to authorised staff only, each Personnel Unit will notify the following units of any new staff, staff departures and internal staff transfers:
    - IT Unit - to update e-mail accounts and access to other IT systems plus arrange issue/return of laptops
    - Finance Unit - to update access to Financial Management System (FMS) and access to other financial systems
    - Accommodation and Services - to disable/limit access i.e. disable swipe card to offices or Department and to arrange issue/return of mobile phones
- Premises are kept secure, especially when unoccupied
- Access to information is restricted to authorised staff in accordance with the Department's Computer and Network Usage Policy and Records Management Policy
- Appropriate facilities are in place for disposal of confidential waste

- Computer systems are password protected
- Personal security passwords are not disclosed to any other individual (including other employees within the Department)
- Staff are required to lock their computers when they leave their work stations. The Department's computer system is set to lock computers if they are not accessed after a pre-set amount of time and a password is required to unlock the computer. At the end of the working day, staff are required to log out of the computer system and to file and lock away any paper files containing personal data
- Information on computer screens and paper files is kept hidden from callers to offices
- Personal data is protected by strong encryption when being stored on portable devices or transferred electronically (including via email)
- Audit logs are kept in relation to changes, additions and deletions to specific data on key ICT systems. Line managers will assess the requirement to monitor access to applications with personal data to ensure the required level of monitoring is in place. Managers to work with IT Unit in relation to this.
- Appropriate data protection and confidentiality clauses are in place in arrangements with any processors of personal data on the Department's behalf. Where third parties are used to process personal data this is covered by contract.

All staff are required to meet these standards and managers must carry out periodic reviews of measures and procedures.

5. Keep data accurate, complete and, where necessary, up-to-date

The Department seeks to ensure that personal data held is accurate complete and up to date.

Every individual has a right to have any inaccurate data rectified or erased.

6. Ensure that data are adequate, relevant and not excessive in relation to the purpose for which they were collected

Personal data held by the Department should be enough to enable the Department to achieve its purpose, and no more. The Department will not collect or keep personal information that is not required for a specific purpose, or ask intrusive or personal questions, if the information obtained in this way has no bearing on the specified purpose for which the personal data is held.

Forms used to collect personal data will state what the data will be used for, who will have access to the data and that the data will be processed in accordance with the Data Protection Acts.

7. Retain data for no longer than is necessary for the specified purpose or purposes

This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the data is being retained. Data should never be kept "just in case" a use can be found for it in the future.

The Department will publish a retention schedule for records which will state how long data will be retained and the reasons for retaining data.

Under the National Archives Act, 1986, the Department requires the permission of the National Archives in order to destroy any records. If there is no reason for retaining personal data, the Department will request permission from the National Archives to destroy this data.

Destruction of data will be carried out in a secure manner in line with the Department's procedures (contact Records Management Unit for details).

8. Give a copy of his/her personal data to an individual on request and in some cases correct the data, block or erase the data where an individual requests

Under Section 3 of the Data Protection Acts an individual, who believes that the Department keeps personal data in relation to them, shall, if he so requests the Department in writing:

(a) be informed by the Department whether any such data is kept, and
(b) if so, be given a description of the data and the purposes for which they are kept, not more than 21 days after the receipt of the request.

Under Section 4 of the Data Protection Acts, on making a written request, any individual about whom personal data is kept on computer or in a relevant filing system is entitled to:

a) a copy of the data
b) a description of the purposes for which it is held
c) a description of those to whom the data may be disclosed and
d) the source of the data unless this would be contrary to public interest.

In addition, the Department will explain to the data subject the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process.

This "right of access" is subject to a limited number of exceptions. The restrictions upon the right of access fall into five groups:

- Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases, in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand, such as the need to

investigate crime effectively and the need to protect the international relations of the State.

- The right of access to medical data and social workers' data is also restricted in some very limited circumstances, to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being. In such circumstances it should be made available to his or her GP, who will then talk them through it.
- Section 4(6) of the Data Protection Act makes special provision for responding to an access request about the results of an examination. "Examination" in this context means any test of knowledge, skill, ability etc., and is therefore not confined to official State examinations. Medical examinations are not covered, though. These special rules increase the time limit for responding to an access request from 40 days to 60 days, and deem an access request to be made at the date of the first publication of the examination results or at the date of the request, whichever is the later.
- The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion except where that expression of opinion was given in confidence.
- The obligation to comply with an access request does not apply where it is impossible for the data controller to provide the data or where it involves a disproportionate effort. For example, if files are archived and are not used for decision–making as part of the day to day operations of the organisation, and retrieval involves disproportionate effort (or perhaps even cost where a storage company is used), then the data could be said to be not readily accessible. In such a circumstance, the data subject would need to be able to identify particular data by file reference or date so that on a reasonable view of things the data could be said to be readily accessible. This restriction on the right to access should have narrow application in practice, the Data Protection Acts require that the right to access be guaranteed and would not appear to allow for this right to be refused outright because it results in a data controller exerting "disproportionate effort".

If an access request is being refused, the reasons for its refusal must be clearly outlined to the data subject (as per exemptions in Sections 4, 5 and 8 of the Data Protection Acts).

It should be noted that where a request is made to a public body by, or on behalf of, a person seeking access to their own personal data under the Freedom of Information Act, this request should also be taken as a request under the Data Protection Acts. This is because a valid Data Protection request does not need to refer to the Data Protection Act. Guidance on how organisations should deal with the overlapping rights of individuals is contained in the Freedom of Information Central Policy Unit Notice Number

23 which is available at http://www.foi.gov.ie/cpu-notices.

Responsibility of Employees

All employees of the Department have a duty to ensure compliance with the principles of Data Protection and undertake to follow the provisions of this Code of Practice. All employees are charged with the responsibility of ensuring that all data that they access, manage and control as part of their daily duties is carried out in accordance with the Data Protection Acts and this Code of Practice. Breaches of the terms and conditions of this Code of Practice may result in disciplinary action by Personnel Unit.

Principal Officers are nominated as data controllers with responsibility to ensure that staff are aware of and meet the required security measures to protect personal data. Corporate Services Section will ensure that information to allow staff and managers to comply fully with this Code of Practice is provided on the Department's Intranet. Data Protection training is included at induction training courses for new staff.

Audits of Procedures

The Internal Audit Unit will, in the course of its programme of audits of units in the Department, assess the adequacy of the control systems in place for the purpose of minimising the risk of any breach of data protection regulations. Audits will include an assessment of the adequacy of the control systems designed, in place and operated by units in the Department for the purpose of minimising the risk of any breach of data protection regulations.

Risks associated with the storage, handling and protection of personal data are included as generic risks in the Department's Risk Register. However, individual units within the Department must assess the risk to data managed and controlled by them and ensure systems and procedures are in place to eliminate these risks.

External audits of all aspects of Data Protection within the Department may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

Role of the Data Protection Commissioner

The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Data Protection Acts and for enforcing obligations upon data controllers (i.e. organisations that store personal information).

The Commissioner maintains a register, available for public inspection, giving general details about the data handling practices of a range of data controllers, such as Government Departments, State Agencies and financial institutions.

The Commissioner has a wide range of enforcement powers, including investigation of Department records and record-keeping practices. Summary proceedings against a data controller for an offence under the Data Protection Acts may be brought and prosecuted by the Data Protection Commissioner. Under Section 31 of the Acts, the maximum fine on summary conviction of such an offence is set at €3,000. On conviction on indictment, the maximum penalty is a fine of €100,000. A data controller found guilty of an offence can, in addition to a fine, be ordered to delete data.

If an individual feels that the Department is not complying with its responsibilities under the Data Protection Acts or the Department fails to respond to a request for access to personal data, then the individual can make a complaint to the Data Protection Commissioner, who will investigate the matter on their behalf.

When responding to an individual's request for access to personal data you should inform them of their right to raise the matter with the Data Protection Commissioner. They can do this by contacting the Commissioner at Canal House, Station Road, Portarlington, Co. Laois (Tel: 057 8684800, Fax: 057 8684757).

When the Department receives a complaint from the Data Protection Commissioner's Office, the Data Controller/Data Protection Officer must acknowledge receipt of the complaint immediately and include the name of the officer appointed to investigate the complaint in the acknowledgement letter. A final reply must issue as soon as possible.

Please see the Data Protection Commissioner website at www.dataprotection.ie for further information.

Protocol for reporting breaches

A data security breach can happen for a number of reasons, including:-

- Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a flood or fire;
- A hacking attack;
- Access where data is obtained by deceiving the organisation that holds it.

If any breaches of this Code of Practice or of the regulations in the Data Protection Acts are committed, a report of the incident must be submitted to the Records Management Unit, through the Principal Officer of the Unit involved. A form for reporting breaches is available on the Department's Intranet or from the Records Management Unit.

All instances of the loss of personal data (except where the data can be considered inaccessible due to proper security) must be reported to the Office of the Data Protection Commissioner where it affects more than a hundred individuals or where it involves any loss of sensitive personal data or personal financial data that could be used to carry out identity theft. All instances of breach of security or loss of personal data must be reported to the Records Management Unit – see policy Data Protection Breach Policy – Records Management Unit will decide which breaches need to be reported to the Data Protection Commissioner's office.

APPENDIX 1 Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of this Code of Practice;

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All Department staff must comply with the provisions of the Data Protection Acts when collecting and storing personal data. This applies to personal data relating both to employees of and individuals who interact with the Department.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Relevant Filing Systems - Any set of information organised by name, PPSN, payroll number, employee number or date of birth or any other unique identifier would all be considered relevant.

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Department.

Access Request – Where a person makes a request to the Department for the disclosure of their personal data under Section 4 of the Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – An individual who is the subject of personal data.

Data Controller - A person who (either alone or with others) controls the contents and use of personal data.

Data Processor - A person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Act places responsibilities on such entities in relation to their processing of the data.

APPENDIX 2 Enforcement of Data Protection Legislation

Data Protection Commissioner

The Data Protection Acts established the independent office of the Data Protection Commissioner. The Commissioner is appointed by Government and is independent in the performance of his/her functions. The Data Protection Commissioner's function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the Data Protection Acts.

The Data Protection Commissioner has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include the serving of legal notices compelling a data controller to provide information needed to assist his enquiries, compelling a data controller to implement a provision in the Act and investigating complaints made by the general public. The Commissioner may authorise officers to enter premises and to inspect personal data held on computer or relevant paper filing systems.

A data controller found guilty of an offence under the Acts can be fined amounts up to €100,000 on conviction and/or may be ordered to delete all or part of a database if relevant to the offence.

Employees of the Department

Where employees of the Department, in the normal course of their duties, become aware that an individual including employees of the Department may be breaching the Acts or have committed or are committing an offence under the Acts, they should report the matter to Data Protection Officer, Records Management Unit, Department of Education and Skills, Marlborough Street, Dublin 1.

Advice/Assistance

All requests for advice and assistance on data protection issues within the Department should be directed to:

Data Protection Officer
Records Management Unit
Department of Education and Skills
Marlborough Street
Dublin 1
Telephone 01 889 6444 or
records_management@education.gov.ie

APPENDIX 3 Applying for Access to Personal Data

(Information on Freedom of Information in the Department of Education and Skills, including application forms, is available on the Department's website at www.education.ie)

AN ROINN OIDEACHAIS AGUS SCILEANNA | DEPARTMENT OF EDUCATION AND SKILLS

Application Form for Data Access (subject access request)

Request for Access to Data under the Data Protection Acts, 1988 and 2003

Before completing this form, read:
Data Protection - Your Rights from the Data Protection Commissioners website

This will help you decide what data is relevant to your needs.

Answer all questions fully, and indicate the appropriate details using an 'X' in the boxes provided.

Complete the form using BLOCK LETTERS

PART ONE: Details of Data Subject

1. Contact Details

Full Name: _____

Address: _____

_____

Contact number: _____

Email address: _____

2. To help locate your personal data, please state the nature of the contacts you have had with this Department (e.g. letters/representations to Minister, submission of application forms, requests for information by letter, email or telephone contact etc.)

_____

_____

3. Please provide any reference numbers relating to your contact Department

_____

_____

PART TWO: Details of request

The Department has a number of data holdings registered with the Office of the Data Protection Commissioner. You can request personal information held under one or more of these data holdings by marking 'X' in the appropriate box (es).

School Staffing and Payroll Services	**Description of personal data**	
Payroll - payment on a fortnightly basis of serving and retired teachers and special needs assistants in primary, voluntary secondary, community and comprehensive schools, a number of serving and retired clerical officers and caretakers in primary and voluntary secondary schools and a number of child-care workers in primary schools. Personal data on ancillary school staff who are employed in schools where a new building is to be provided via Public Private Partnership Personnel and payroll services for Visiting Teachers for Traveller children and children with a visual or hearing impairment. Administration and regulation of pension matters of education sector staff Industrial relations and employment legislation issues Secondment of Irish teachers to European schools	Name Contact details Date of birth Gender Marital status PPS number, Payroll number, teacher ID number, pensioner ID number Bank account details Details of pay and service history including qualifications, sick leave and other leave or absence details Names of deduction agencies with whom the person has agreed to have deductions made from salary Trade Union membership Medical assessment Garda vetting Photo ID in the case of Visiting Teachers Nature of complaint in relation to industrial relations issues	
Services to Schools and VECs	**Description of personal data**	
Assist school authorities and VECs by providing policies and supports in relation to their role	Personal data held in relation to administration of schemes for teachers and Special Needs	

as employers of teachers and Special Needs Assistants Administration of services in respect of Schools. Operating an inspection and evaluation programme, including school, teacher and subject inspection, programme inspection and Whole School Evaluation	Assistants. Details of management, teaching and non teaching staff in schools, including Vocational Education Committees Details of pupils required in connection with the provision of financial support and for policy objectives Details held for the purpose of administration of schemes or the provision of services to Schools. Details of personal information in relation to appeals and complaints, including child protection allegations. Details of members of educational organisations. Details of personal information in relation to the administration of grant aid schemes to parents and pupils. Personal data held - Name, address, Date of Birth, Teacher Number, PPS number and qualifications.	
Early Childhood, Special Needs and Social Inclusion Services	**Description of personal data**	
Assessment of suitability of those nominated by the National Voluntary Childcare Organisations for the role of Síolta co-ordinators Provision of a school transport service for students at primary and post primary levels. Provision of education support services for children with special educational needs.	CV data including name, address, educational qualifications and relevant work experience Name, address, date of birth, transport requirements. Names, addresses, PPS Numbers, dates of birth, education data, medical reports, diagnostic and assessment reports.	

Provision of educational psychological service to primary and post primary schools in conducting educational psychological assessment on individual pupils.	Pupils name, address, (parents names and addresses), date of birth, gender, phone number, reason for referral, source of referral, NEPS action, hypotheses, results of IQ and other tests administered, recommendations, consultation, interview notes and assessment reports.	
Scheme for Commissioning Psychological Assessment (SCPA) - a panel of private practitioners is utilised by school and paid for by NEPS.	Psychologist name, address, contact details, record of Garda clearance, scheme application form, details of payments, hard copy of assessment reports.	
Provision of personal records to former residents of industrial and reformatory schools, to the Commission to inquire into child abuse and to the Residential Institutions Redress Boards.	Archival records relating to the administration of the old industrial and reformatory schools in addition to 13,000 pupil files containing personal information relating to former residents held for the purposes of providing information to former residents and to the Commission to Inquire into Child Abuse.	
Management of the response in cases where litigation has been initiated or threatened against the Minister on behalf of children and adults with special educational needs who are claiming the education provided to them is inadequate or who are seeking different education than that provided by the State	Names, addresses, Dates of Birth, Education Data, Medical Reports, Diagnostic and Assessment Reports	
Administration of services in High Support Special Schools, Youth Encounter Projects and Line Projects.	Names, addresses, date of birth, assessment reports	
Provision of education support services by the Visiting Teacher Service in respect of Traveller children and Children with a	Personal data, on families and children for the purpose of managing caseloads and case files including:	

visual or hearing impairment. Confidential records of child protection and welfare referrals to HSE and internal referrals to the Department of Education and Skills Schools Division	Names of children, parents/guardians, gender of children, dates of birth of children, contact details Assistive technology assigned to the child School attendance and examination results Details of referrals, medical and other relevant reports. In relation to the child: Name of child and parents/guardians, Gender, Date of birth, Contact details for child and parents/guardians, Care and custody arrangements, Household composition, Details of concerns, Suspicions, Allegations, Incidents In relation to the person allegedly causing concern for the child: Name, Address, Age, Gender, Occupation and Relationship to the child. In relation to the person reporting their concerns and completing the form (both included if different); Name, Address, Telephone number, Occupation, Nature and extent of contact with child/family	
Further and Higher Education Services	**Description of personal data**	
Funding and development of student support services to enable students undertake higher and further education programmes. Some records of staff and former	Names, addresses, dates of birth, PPS numbers, income details and examination results provided by students and their parents/guardians or spouses in order to process applications for financial support and scholarships. Name, college, grade,	

staff of Institutes of Technology are retained by the Department as a requirement of relevant legislation.	qualifications etc.	
WorldSkills Competition	Application forms in respect of participants and examiners containing personal data.	
Identification of teachers claiming payments for Locally Devised Assessments	PPS number, Name	
International Programmes i.e., Third level expert exchanges organised under cultural arrangements; Post Graduate scholarships application dossiers and Undergraduate and Post Graduate applications to go as English Language Assistants to schools in Germany, Austria, Italy, France and Spain.	Personal data may include: Name and contact details Date of birth Nationality Bank account details Curriculum vitae - educational and work background, achievements In some cases e.g. applicants to Russia, copy of last page of passport	
Policy Advice, Development and Review Services	**Description of personal data**	
Applications for funding for research and development project.	Name, address, date of birth, employment history.	
Corporate Services	**Description of personal data**	
Details in respect of staff of the Department	Name, address, date of birth, next of kin, dependants, career history, sick leave records, annual leave records, performance management, PPS number, salary details and details of payments of travel and subsistence allowances.	
Correspondents with the Department's Press Office, Offices of the Minister and Ministers of State, Office of the Secretary General, Regional Office Service and Corporate Services.	Personal data held could include name, address, date of birth, gender, PPS number, teacher number and pupil number. Parents name(s), nature of and outcome of complaint, query	
Service providers	Name, address, VAT and tax numbers and bank details.	

This access request must be accompanied with a copy of photographic identification e.g., passport or drivers licence.

PART THREE: Declaration

I declare that all the details I have given in this form are true and complete to the best of my knowledge.

Signature of Applicant …… Date: ……

Please return the completed form to:
Data Protection Officer
Records Management Unit
Department of Education and Skills
Marlborough Street
Dublin 1.
Email: records_management@education.gov.ie Telephone: 01 889 6444

Responding to Requests

When a valid request is received, the Organisation must reply within 40 days[1], even if personal data is not held.

Useful Contacts

Data Protection Commissioner's Office,
Phone: 1890 252231,
http://www.dataprotection.ie
info@dataprotection.ie

[1] 21 days if the request is to be informed if any personal data is held and to be given a description of the data and the purposes for which they are kept (Section 3 of the Data Protection Acts)