DATA PROTECTION POLICY

VERSION 1.0

DATA PROTECTION POLICY

Table of Contents

1.Introduction

The Department of Education and Skills is a Department of the Government of Ireland. The Department's mission is:

to facilitate individuals, through learning, to achieve their full potential and contribute to Ireland's social, cultural and economic development.

The Department provides a policy, legislative and funding framework for, and supports, education and skills development in early childhood settings, primary and post primary schools, higher education institutions, further education providers, and adult and second chance education. It provides a range of services directly for the sector. In this, the Department is supported by a number of agencies, details of which are available on the website www.education.ie .

The Department is not involved in the direct delivery of education, rather, it works in partnership with schools and other education and training providers, parents, students, patrons, staff and communities to achieve its objectives. The Department's role is reflected in the staff complement of just under 1300 which is of a limited size in comparison with the scale of the sector and its budget.

The Department is committed to protecting the rights and privacy of individuals in accordance with both European Union and Irish data protection legislation. The Department needs to lawfully and fairly process personal data about employees, clients, suppliers and other individuals in order to achieve its mission and functions.

The data protection legislation confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how the Department seeks to process personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

The EU General Data Protection Regulation (GDPR EU 2016/679) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. The GDPR will be enforced from 25th May 2018. This version of the Department policy has been updated to reflect the GDPR.

2.Scope & purpose

This policy applies to all of the Department's personal data processing functions in relation to identified or identifiable natural persons, including those performed on clients, employees, suppliers' and any other personal data the Department processes from any source.

Personal data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

This policy should be read in conjunction with other relevant Department policies, Portable and Mobile Devices, Data Breach and Subject Access Requests. The Department may supplement or amend this policy by additional policies and guidelines from time to time. Please refer to the Department's' Data Protection pages on the internet for further details.

3. Responsibility for this policy

The Minister, Junior Ministers, Secretary General, Deputy Secretary and Assistant Secretaries of the Department are committed to compliance with all relevant EU and Irish laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information Department collects and processes.

Senior Officers, Assistant Secretaries and Principal Officers are responsible for ensuring that this policy is implemented in their respective Divisions. Principal Officers and equivalent grades are the designated data controllers for their areas of responsibilities, where the section collects, stores or processes any personal data.

Managers at all levels will be accountable for being able to demonstrate that this policy has been implemented.
All members of staff have a responsibility to comply with Department's' data protection policies.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles set out in relevant legislation. The Department's policies and procedures are designed to ensure compliance with the following principles:-

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – the Department processes personal data where it is necessary for

- *the performance of a task carried out in the public interest or in the exercise of official authority vested in the Department;*
- *compliance with a legal obligation;*
- *the performance of a contract;*
- *the protection of the vital interests of an individual or another person;*
- *processing undertaken on the basis of consent;*
- *the purpose of legitimate interests pursued by the Department as an organisation as opposed to carrying out public tasks as a department of the Irish government.*

Tasks in the public interest or exercise of official authority

The Department processes personal data in carrying out tasks in the public interest or in the exercise of official authority to the extent that such processing is necessary and proportionate for

- the performance of functions conferred under enactment (primary or secondary legislation) or by the Constitution (e.g. government decision, monies voted by the Oireachtas) or
- the administration (e.g. by departmental circular) of non-statutory schemes, programmes or funds where the legal basis for such administration is a function of the Department conferred by or under an enactment or by the Constitution.

The statutory functions of the Department are provided for in the Education Act, 1998 and other legislation.

Under section 7 the Education Act 1998 the function of the Minister is to provide for education and to provide support services to recognised schools, centres for education, students, including students who have a disability or who have other special education needs, and their parents as the Minister considers appropriate.

Under section 24 of the Education Act 1998 the Minister in concurrence with the Minister for Public Expenditure and Reform also determines the terms and

conditions of employment of teachers and other staff of a recognised school, appointed by the boards and who are to be, remunerated out of monies provided by the Oireachtas.

A list of some relevant legislation is available here https://www.education.ie/en/The-Education-System/Legislation/

Under section 266 of the Social Welfare Consolidation Act, 2005 provision is made for specified bodies as identified in the schedule attached to that Act to share personal data with the Department.

Legal obligation

Processing of personal data undertaken by the Department may also rely on legal obligations e.g. deductions under the Tax and Social Welfare legislation. The Department is subject to the National Archives Act, 1986 and therefore is required to retain records which may contain personal data for the purpose of archiving.

Contract

The Department may also process personal data necessary for the performance of a contract for services or goods or in respect of contracts of employment with respect to its own employees.

Vital interest of an individual or others

The Department may on occasion process personal data where it is necessary in order to protect the vital interests of an individual or of another person. This type of processing may be required for child welfare or protection purposes.

Consent

As a large public body the Department does not rely on consent as a legal basis other than for limited purposes where the processing is optional and where the individual is freely able to give his/her consent for processing by the Department, e.g. inclusion in an e-mail distribution list, surveys.

Legitimate interest

As a public authority the Department does not rely on legitimate interest when carrying out its public tasks. The Department does however rely on the use of legitimate interest where processing of personal data is related to the operation of the organisation, e.g. the operation of CCTV for the purposes of security and safety of persons using its facilities.

Fairly – in order for processing to be fair, the Department has to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the Department will provide the required information to data subjects at the time personal data is collected. The Department will ensure that the information provided is detailed and specific, and that such notices are understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. In order to balance the requirements above, the Department may implement appropriate policies to make information available on its website or from schools and other educational organisations. The information provided must include information about personal data collected both directly from the data subject and from other sources. The Department may adopt standardised icons in the future.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes

.

The Department will collect and process personal data only for the purposes for which it is collected and purposes which are compatible with those purposes. The Department staff must be alert to requests for processing of personal data for purposes for which it was not collected, no matter how related the processing may appear. Processing should only continue after an assessment of the impact of the new processing. This assessment may be done as a data protection impact assessment, please see section 6.6 below.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)

The Department will ensure that in designing methods of data collection, whether online, or through data collection forms, that only the personal data required to identify the data subject(s), and provide the service or programme will be processed. The Department undertakes regular reviews of the data requested to ensure that the amount of personal data collected is minimised.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

All data subjects have a right to ensure that their data is accurate and complete. The Department needs data which is accurate for the purpose for which it will be used. All data collection procedures should be designed to ensure that reasonable steps are taken to update personal data where new data has been provided. Where a correction is made to personal data at the request of the data subject all changes to their personal data should be

shared with each third party with whom the previous data had been shared, unless this is impossible or requires disproportionate effort.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

The Department will implement appropriate policies and procedures to ensure that personal data is retained only for the minimum period required for the purpose or purposes. This may be done by destroying the personal data, by anonymization or any other appropriate method.

4.6 Personal data must be processed in a manner that ensures appropriate security

The Department will implement appropriate technical and organisation measures to ensure that appropriate security of the processing of personal data is implemented.

4.7 Accountability for demonstrating compliance

The Department will ensure that it maintained adequate records of its processing and evidence that it has complied with this policy and related policies and procedures. Responsibility for collecting and maintaining the evidence is with Management. See section 3 of this policy for further guidance.

5. Rights of Individuals whose data is collected

The Department will design and maintain appropriate policies, procedures and training to implement the following data rights of data subjects.

5.1 Right of access by the data subject

The Department will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled in accordance with the legislation.

5.2 Right to rectification

The Department is committed to holding accurate data about data subjects and will implement processes and procedures to ensure that data subjects can rectify their data where inaccuracies have been identified.

5.3 Right to erasure (right to be forgotten)

The Department processes personal data it collects because there is a legal basis for the processing. Where the Department receives requests from data subjects looking to exercise their right of erasure then the Department will carry out an assessment of whether the data can be erased without affecting the ability of the Department to provide future services to the data subject or to meet it statutory obligations for example under the National Archives Act, 1986.

5.4 Right to restriction of processing

The Department will implement and maintain appropriate procedures to assess whether a data subjects request to restrict the processing of their data can be implemented. Where the request for restriction of processing is carried out then the Department will write to the data subject to confirm the restriction has been implemented and when the restriction is lifted.

5.5 Right to data portability

The Department processes personal data its collects because there is a legal basis for the processing. Where the Department has collected personal data on data subjects by consent or by contract then the data subjects have a right to receive the data in electronic format to give to another data controller. It is expected that this right will apply only to a small number of data subjects.

5.6 Right to object (Art.21)

Data subjects have a right to object to the processing of his or her personal data in specific circumstances. Where such an objection is received, Department will assess each case in its merits.

5.7 Right not to be subject to automated decision making (Art.22)

Data subjects have the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant

effect concerning him or her. At present there is no automated processing within the Department if it future such processing is commenced the Department will ensure that where systems are implemented then an appropriate right of appeal is available to the data subject.

5.8 Right to complain

The Department will implement and maintain a complaints process whereby data subjects will be able to contact the Data Protection Officer. The Data Protection Officer will work with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject will be informed of their right to bring their complaint to the Data Protection Commissioner and their contact details.

6. Responsibilities of the DES

The DES has responsibility for the following

6.1 Ensuring appropriate technical and organisational measures

The Department will implement appropriate technical and organisational measures to ensure and be able to evidence that it protected personal data always.

6.2 Maintaining a record of data processing

The Department will maintain a record of its data processing activities (ROPA) in the manner prescribed by Regulation. The record will be reviewed and signed off by designated data controller (i.e. Principal Officer), not less than on an annual basis.

6.3 Implementing appropriate agreements with third parties

For the sharing of personal data by the Department with a third party to takes place there must be a legal basis and the sharing must be transparent. Where a legal basis for sharing exists the Department will implement appropriate agreements, memoranda of understanding, bilateral agreements and contracts (collectively "agreements") with all third parties with whom it shares personal data to identify the roles and respective responsibilities of each party. The term third parties is meant to include other agencies, departments of the Irish Government and schools and other educational organisations. All such agreements shall be implemented in writing prior to the commencement of the transfer of the data. The agreement shall specify the purpose of the transfer, the requirement for adequate security, right to terminate processing, restrict further transfer to other parties, and that ensure that responses will be given to requests for information and the right to audit.

6.4 Transfers of personal data outside of the European Economic Area

The Department will not transfer the personal data of its data subjects outside of the European Economic Area unless an adequate level of protection is ensured or other measures as required by the GDPR are in place.

6.5 Data protection by design and by default

The Department will implement processes, prior to the time of determining the means of processing as well as when actually processing, to implement appropriate technical and organisational measures to implement the data protection principles set out in Section 4 and integrate necessary safeguards into the processing to meet GDPR requirements.

6.6 Data protection impact assessments

The Department will implement procedures and documentation whereby all new types of processing, in particular using new technologies, that result in a

high risk to the rights and freedoms of its data subjects shall carry out a data protection impact assessment. As part of this process, a copy of the impact assessment shall be shared with the Department's' Data Protection Officer. Where the Department is unable to identify measures that mitigate the high risks identified then the Department will consult with the Data Protection Commissioner prior to the commencement of processing.

6.7 Personal data breaches

The GDPR (Article 4(12) defines a 'personal data breach' as meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. (e.g. the most common breach incidents that can occur are correspondence issuing to an unauthorised third party). The Department deems any loss of personal data in paper or digital format to be a personal data breach.

The Department will develop and maintain a protocol for dealing with personal data breaches. This protocol will establish the methodology for handling a personal data breach and for notification of the breach to Data Protection Commissioner and to data subjects where this is deemed necessary.

6.8 Freedom of Information

The Department maintains a separate policy to ensure compliance with FOI. The Department will maintain procedures to ensure that requests for personal data are correctly fulfilled under either data protection legislation or FOI legislation.

6.9 Governance

The Department will monitor compliance with relevant legislation on data governance and protection. The Department at a senior management level will

- Determine data governance policies for the Department
- Determine records management policies for the Department
- Determine metrics for monitoring & reporting key data protection statistics
- Receive regular reports of data protection activities from Department Divisions
- Receive regular reports from the Data Protection Officer
- Review data protection impact assessments and approve or not the design of data protection elements of projects
- Instigate investigations of data protection matters of interest
- Arrange audits, or similar, of Department units for compliance with this policy
- And other such activities relating to the Department compliance with EU & Irish Law in the area of data protection.

7. The Data Protection Officer's Responsibilities

The Department will appoint a Data Protection Officer. The Data Protection Officer will report to the highest level of senior management within the Department concerning the tasks allocated to them. The responsibilities of the Data Protection Officer will include the following

i. Keeping the Management Board and where designated sub-committees of the management board updated about data protection responsibilities, risks and issues

ii. Act as an advocate for data protection within the Department

iii. Monitoring compliance with the relevant data protection legislation.

iv. Monitoring that all data protection policies and policies are reviewed and updated on a regular basis

v. Monitoring that the Department provides appropriate data protection training and advice for all staff members and those included in this policy

vi. Providing advice where requested as regards the data protection impact assessments and monitoring that such assessments are completed to an appropriate standard

vii. Provide advice on data protection matters from staff, board members and other stakeholders

viii. Responding to individuals such as clients and employees who wish to know which data is being held on them by the Department

ix. Monitoring that appropriate data processing agreement are put in place with third parties that handle the Department's ' data and ensuring that reviews are carried out of third parties on a regular basis

x. Monitoring that the record of data processing activities (ROPA) is updated regularly.

xi. Acting as a contact point and providing cooperation with the Data Protection Commissioner

8. Responsibilities of staff and similar parties

Anyone who processes personal data on behalf of the Department has a responsibility to comply with this data protection policy. Detailed advice on how to achieve this is available on the Department's internal website.

8.1 Training and awareness

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Completion of training is compulsory.

Also, staff are continuously reminded of data protection obligations through annual data protection obligations for signing; regular poster campaigns; e-mails to staff; resources on the Department's intranet site; regular awareness weeks; annual obligations notice.

8.2 Consequences of failing to comply

The Department takes compliance with this policy very seriously. Failure to comply puts both the staff member and the Department at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under the Civil Service Disciplinary Code.

9. Where to go if you have queries about the data protection policy

The Department has resources at its internet site www.education.ie and you should refer to these in the first instance.

If you cannot find the answer to your query on the website then you can contact

The Data Protection Officer
Data Protection Unit
Cornamaddy
Athlone
Co. Westmeath
N37 X659

090 648 3908

dpo@education.gov.ie

This policy comes into effect on 25 May 2018.

The next review of this policy is scheduled for May 2019.

Disclaimer

This document has been produced for the purposes of general information only. The contents of this document do not constitute legal advice on any particular or general matter. If you require legal advice you should contact your legal advisor.