Department for Education

Data Protection Policy

Version 4

Data Protection Office, Data Directorate

March 2023

Contents

[1] See referenced and relevant documents section for more information

Version Control

Version	Date	Author	Change Description
v1.0	27/10/2021	Office of the Data Protection Officer	Draft for review by Data Policy Community.
v2.0	13/12/2021	Office of the Data Protection Officer	Review by DfE Data Governance Board.
v3.0	15/12/2021	Office of the Data Protection Officer	Final version for publication.
v3.1	30/03/2022	Office of the Data Protection Officer	Updated Links
V4	15/03/2023	Office of the Data Protection Officer	Updated to reflect DfE Policy on Policies

This policy was last reviewed March 2023 and will be reviewed before March 2024 or when the Data Protection and Digital Information receives Royal Assent, whichever is sooner.

Document Review

This policy must be reviewed annually (or more frequently as determined by the DPO) and revised based on changes in regulations, DfE's objectives, strategies, and technological advancements. Any revisions to be approved by the DfE Data Governance Council.

Referenced Documents

All Data Management frameworks, policies and standards can be located on the DfE Gateway to Data Compliance Data Policies, Standards & Tools page.

Terminology

Term	Meaning/Application
Shall	Used to state a Mandatory requirement of this policy
Should	Used to state a Recommended requirement of this policy
May	Used to state an Optional requirement of this policy

[1] See referenced and relevant documents section for more information

1. Executive summary

To meet our obligations, we must put in place appropriate and effective measures to make sure we comply with data protection law. DfE staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation.

This policy provides a framework for ensuring that the DfE meets its obligations under the UK General Data Protection Regulation (UK GDPR) and associated Data Protection legislation including the Data Protection Act (DPA 2018). It applies to all the processing of personal data carried out by the DfE and its Agencies, where the department is the data controller. It includes processing carried out by joint controllers, contractors and processors.

1.1 Benefit

This policy aims to ensure compliance with data protection legislation, guided by the seven data protection principles that require:

1. **Lawfulness, fairness and transparency** – data shall be processed lawfully, fairly and in a transparent manner
2. **Purpose limitation** – data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. **Data minimisation** – data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. **Accuracy** – data shall be accurate and, where necessary, kept up to date
5. **Storage limitation** – data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. **Integrity and confidentiality (security)** – data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
7. **Accountability** - the accountability principle[1] requires DfE to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data.

1.2 Scope

This policy applies to all personal data and special categories of personal data processed by DfE and as defined under the UK General Data Protection Regulation (UK GDPR).

[1] See referenced and relevant documents section for more information

1.3 Target Audience

This policy sets out to staff, contractors and stakeholders, including third party suppliers, the approach the DfE will take to achieve and maintain data protection compliance. `

1.4 Approval and Governance

All data protection documentation including Policies, Standards and Frameworks are owned by DfE Data Protection Officer.

All related data policies and data standards can be located on the intranet: Gateway to Compliance - Data Policies, Standards & Tools[1].

1.5 Contact

For any enquiries related to this policy document please contact the DfE Data Protection team: dataprotection.office@education.gov.uk

[1] See referenced and relevant documents section for more information

2. Data Protection Policy

2.1 Policy Statements

2.1.1 Compliance with data protection principles

The Department for Education implements appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. We do this by applying adequate resources and controls to document UK GDPR compliance, DfE:

- **Shall** appoint a suitably qualified Data Protection Officer (DPO) and ensure that they have adequate resources to conduct their role[1]
- **Shall** implement Privacy by Design[1] when processing personal data, we will ensure data protection risks are taken into account throughout the data lifecycle. This means assessing and implementing appropriate technical and organisational measures and procedures from the outset to ensure the processing complies with the law and protects the rights of the data subjects.
- **Shall** ensure that only personal data which are necessary for each specific purpose are processed.
- **Shall** ensure that only the minimum amount of personal data is collected and processed for a specific purpose
- **Shall** ensure the processing is limited to that necessary for each purpose
- **Shall** ensure the data is stored no longer than necessary and access is restricted to that necessary for each purpose. The legislation does not impose a strict limit on periods of retention for any data and acknowledges that personal data can be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The decision on how long to retain data shall be based on the DfE retention policy and in consultation with the DfE Records Management team[1].
- **Shall** complete a full Data Protection Impact Assessment (DPIA)[1] where processing presents a high risk to the rights and freedoms of data subjects. A DPIA screener **shall** be carried out for all new processing of personal data. If after the screener is assessed and processing is identified as high risk, a full DPIA shall be completed. If the full DPIA has a high level of residual risk or the processing is novel or contentious, the department will consult with the ICO.
- **Shall** integrate data protection into our policies, processes and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing Activities (RoPA)[1] and records of Personal Data Breaches

[1] See referenced and relevant documents section for more information

- **Shall** raise awareness, provide support and Training[1] staff on how to comply with Data Protection Law and keeping a record of training completed
- **Shall** regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvements
- **Shall** report any losses or suspected breaches[1] of personal data to the Information Commissioner within 72 hours of becoming aware of the breach, if required. Reporting to the ICO **MUST** only be undertaken by the Data Protection Officer or the DPO team on their behalf. When the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we are required by law to notify the affected individuals without undue delay.
- Adequate time **shall** be given to all staff for formal training on data protection, policies and standards. The level of training required will be dependent on the role and may require external courses/certification to be undertaken. The Office of the Data Protection Officer has developed a mandatory annual training programme. All staff shall complete the mandatory training. This will familiarise users with the range of data policies to develop a clear understanding and to make the necessary operational updates to their procedures.

2.1.2 Data Subject Rights

Individuals have rights[1] in relation to the way we handle their personal data. These include:

- Right to be informed about the collection and use of personal data.
- Right to access and receive a copy of written or recorded (audio and video) personal data, and other supplementary information.
- Right to rectification to have inaccurate personal data rectified, or completed if it is incomplete
- Right to erasure of personal information in certain circumstances
- Right to restrict processing of personal data in certain circumstances
- Right to object to processing of personal data in certain circumstances
- Rights related to automated decision-making including profiling. Individuals have the right not to be subject to a decision based solely on automated processing, including profiling
- Right to complain

The lawful basis for your processing can also affect which rights are available. For example, some rights will not apply[1]:

[1] See referenced and relevant documents section for more information

	Right to erasure	Right to portability	Right to object
Consent			X But right to withdraw consent
Contract			X
Legal obligation	X	X	X
Vital interests		X	X
Public task	X	X	
Legitimate interests		X	

2.2 Roles & Responsibilities

The key roles involved in DfE's Data Protection are as follows:

Data Protection Officer (DPO):

- Is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR and making recommendations to improve compliance.
- Is appointed on their abilities, experience and knowledge
- Has the right to challenge the department on their processing and data protection activities is not compliant with the law

Senior Information Risk Owner (SIRO):

- Owns the overall risk arising from the processing of personal data by the DfE.
- Accountable for the management of assets within DfE
- Accountable for managing access controls for accessing assets
- Ensuring all staff receive appropriate information management training for their role
- Acting as an escalation point for Information Asset Owners (IAOs)
- Reporting to the Accounting Officer

Office of Data Protection Officer team:

- Has delegated authority from the DPO in discharging their responsibilities under their function
- Responsible for issuing, reviewing and communicating corporate data protection guidance and procedures to DfE staff

[1] See referenced and relevant documents section for more information

- Responsible for issuing, reviewing and communicating corporate data protection training to DfE staff
- Responsible for compliance with data protection and implement solutions to ensure we take a privacy by design approach and adhere to data protection legislation
- Leads on Data Subject rights and ensuring transparency when dealing with data subjects

Departmental Records Officer:

- leads on departmental compliance with the Public Records Act and related legislation
- ensuring that information worthy of historical preservation is identified and personal data is protected when transferred to The National Archives
- Engages with business areas to ensure that they are implementing relevant retention and disposal policies and storing information in appropriate repositories.

Information Asset Owners (IAOs):

- IAOs have local responsibility for ensuring data protection compliance in relation to their information assets
- Responsible for ensuring all information assets containing personal data are recorded and updated on the Information Asset Register (IAR).
- Responsible for ensuring personal data processing activities are recorded and updated on the Record of Processing Activity (RoPA).

Information Asset Managers (IAMs):

- Support IAOs in complying with their duties regarding the processing of personal data.

Record of Processing Activity (RoPA) owner

- RoPA owners have local responsibility for ensuring personal data processing activities are recorded and regularly reviewed on the RoPA and carry out data protection compliance in relation to their data processing

DfE Staff:

- **Shall** only have to access to personal data if they need it for their work
- **Shall** not share personal data without adherence to DfE's data sharing guidance
- **Shall** complete the mandatory annual training to help them understand their responsibilities when handling personal data and complying with data protection law
- **Shall** keep all personal data secure, by taking sensible precautions and following the departmental policies, standards and procedures

[1] See referenced and relevant documents section for more information

- **Shall** regularly review and update the data they are responsible for. If data is no longer required, it shall be deleted and disposed of.
- **Shall** request help from their line manager or the Office of the Data Protection Officer if they are unsure about any aspect of Data Protection.
- If you suspect a data breach, you **shall** report it through the online Reporting a Security Incident[1] form to the DfE security team.

Further guidance can be found on the Office of the Data Protection Officer[1] pages on the Intranet.

3. Adherence to Policy

Adherence to this policy will be measured as follows:

- Governance KPI measures and data protection reporting, including:
  - Reporting on completed mandatory annual training
  - Review of Data Protection Impact Assessments (DPIAs) and Record of Processing Activities (RoPA) to review personal data processing across DfE and its agencies
  - Personal data incident/personal data breach reporting
  - Information rights reporting
- GIAA Internal Audits will periodically be carried out

Non-adherence to DfE policies and procedures may lead to disciplinary action.

[1] See referenced and relevant documents section for more information

Referenced and Relevant Documents

Referenced Doc	Location
Accountability Principle - GDPR	Accountability principle
DfE Data Protection Impact Assessment (DPIA)	Data Protection Impact Assessment
DfE Data Protection Officer	Data Protection Officer
DfE Gateway to Data Compliance	Gateway to Compliance - Data Policies, Standards & Tools
DfE Information Rights Requests	Individual Rights Requests (IRRs)
DfE Mandatory Training	DfE Mandatory & Required Learning
DfE Office of the Data Protection Officer	Office of the Data Protection Officer
DfE Privacy by Design	Data Protection by design
DfE Privacy Notices	Privacy Notices
DfE Records Management team	DfE Records Management team
DfE Record of Processing Activity (RoPA)	Record of Processing Activities
DfE Retention and Disposal Schedules	DfE Retention and Disposal Schedules
DfE Security incident reporting	Reporting a Security Incident
Lawful basis for processing (ICO guidance)	Lawful basis for processing | ICO
Personal Data Breach Management	Personal Data Breach Management
Storage limitation (ICO guidance)	Principle (e): Storage limitation | ICO

[1] See referenced and relevant documents section for more information

Document Glossary

Acronym/Name	Definition
Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes
Data Controller	The natural or legal person or organisation which, jointly or with others, determines the purposes and means of the processing of personal data. For the purpose of this Policy, it is the Department for Education (including the Education and Skills Funding Agency, Standards and Testing Agency, Teaching Regulation Agency). Some of the department's Arm's Length Bodies are data controllers in their own right, e.g. Ofqual, Ofsted and Student Loan Company.
Data Processor	An individual person or an organisation which uses ("processes") the personal data on behalf of the data controller. Where the data processor and data controller are in different organisations, a contract is required to legally define roles and responsibilities. Processors are third parties who are working under a legally binding contract for a controller and only process personal data under written instruction of that controller.
DPA 2018	Data Protection Act 2018 The DPA 2018 sets out the framework for data protection law in the UK. It updated and replaced the Data Protection Act 1998, and came into effect on 25 May 2018. It was amended on 1 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.
DPIA	Data Protection Impact Assessment - An impact assessment to help identify and minimise project data protection risks.
DPO	Data Protection Officer - A person in an organisation who is responsible for ensuring we comply with Data Protection. This is a legal requirement in a Government Department.
Freedom of Information (FOI) Request	Anyone has the right to request recorded information which is held by public authorities. This is distinct from a request for access to personal data, which is called a Subject Access Request (SAR).
ICO	Information Commissioner's Office - Supports the work of the Information Commissioner as the UK regulator for Information Rights regulation including the Data Protection Act. The ICO has powers to investigate, fine or bring legal action in the case of serious breaches.
Personal data	Personal data means any information relating to an identified or identifiable natural person. Examples of personal data: • a name and surname; • a home address; • an email address such as name.surname@company.com; • an identification card number; • an Internet Protocol (IP) address (in some cases); • ID card number
Processing Personal Data	Processing means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction)
ROPA	Record of Processing Activity - A record of personal data processing activities to demonstrate compliance with UK GDPR.

[1] See referenced and relevant documents section for more information

Acronym/Name	Definition
Special Category data	Special category data is personal data that needs more protection because it is sensitive. The UK GDPR defines special category data as: • personal data revealing **racial or ethnic origin**; • personal data revealing **political opinions**; • personal data revealing **religious or philosophical beliefs**; • personal data revealing **trade union membership**; • **genetic data**; • **biometric data** (where used for identification purposes); • data concerning **health**; • data concerning a person's **sex life**; and • data concerning a person's **sexual orientation**.
UK GDPR	The United Kingdom General Data Protection Regulation - Based on EU GDPR, is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

[1] See referenced and relevant documents section for more information

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Follow us on Twitter:
@educationgovuk

Like us on Facebook:
facebook.com/educationgovuk