Data Protection Policy

Please note that this is an interim precedent document and may be subject to amendment by the Education Authority in due course.

EXECUTIVE STATEMENT

At the Education Authority (EA), we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

We will review and update this data protection policy (the "Policy") regularly in accordance with our data protection obligations.

Any queries in relation to this Policy or any of the matters referred to in it should be submitted to our Data Protection Officer (DPO) who can be contacted at the Education Authority, 40 Academy Street, Belfast, BT1 2NQ, by telephone at 028 8241 1300 or by email at dpo@eani.org.uk.

The following policies, procedures and documents are also relevant to this Policy:

- Data Breach Management Procedure
- Subject Access Request Procedure
- Public Record Office (NI) Record Management Good Practice Guidance

DATA PROTECTION POLICY

1. Scope

1.1. EA is subject to the General Data Protection Regulation (GDPR) which imposes obligations on EA as a data controller in relation to the protection, use, retention and disposal of Personal Information. This Policy sets out the procedures that are to be followed when dealing with Personal Information and applies to all Personal Information processed by or on behalf of EA.

1.2. You must read this Policy because it gives important information about:

1.2.1. the data protection principles with which EA must comply;

1.2.2. what is meant by Personal Information and Special Category Data;

1.2.3. how we gather, use and (ultimately) delete Personal Information and Special Category Data in accordance with the data protection principles;

1.2.4. where more detailed Privacy Information can be found, e.g. about the Personal Information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;

1.2.5. your rights and obligations in relation to data protection; and

1.2.6. the consequences of our failure to comply with this Policy.

1.3. Please refer to EA's privacy notices which are available on our website at www.eani.org.uk/privacy and, where appropriate, to other relevant policies including in relation to data breach management, subject access requests and document retention and disposal which contain further information regarding the protection of Personal Information in those contexts.

2. Data Protection Principles

2.1. GDPR sets out the following principles with which any party handling Personal Information must comply. All Personal Information must be:

2.1.1. processed lawfully, fairy and in a transparent manner;

2.1.2. collected for specified, explicit and legitimate purposes only, and will not be further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

2.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4. accurate and, where necessary, kept up to date and take reasonable steps to ensure that inaccurate Personal Information are deleted or corrected without delay;

2.1.5. kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed; Personal Information may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the individual; and

2.1.6. processed in a manner than ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Lawful, Fair and Transparent Processing

3.1. EA will, before any processing of Personal Information starts for the first time, and then regularly while it continues:

3.1.1. process the Personal Information on at least one of the following bases:

3.1.1.1. **Consent:**

- the individual has given their express agreement to the processing of their Personal Information for one or more specific purposes;
- parental consent will be obtained for any child aged under 13 years old or for children aged over 13 who are not considered capable of giving consent themselves.

3.1.1.2. **Contractual**:

- the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

3.1.1.3. **Legal Obligation**:

- the processing is necessary for compliance with a legal obligation to which the Authority is subject;

3.1.1.4. **Vital Interests**:

- the processing is necessary for the protection of the vital interests of the individual or another natural person; or

3.1.1.5. **Public Interest**:

- the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

3.1.1.6. **Legitimate Interests**:

- the processing is necessary for the purposes of legitimate interests of EA or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual, in particular where the individual is a child.

3.1.2. except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

3.1.3. document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles;

3.1.4. include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices which can be found on our website at www.eani.org.uk/privacy.

3.1.5. where Special Category Data is processed, identify a lawful special condition for processing that information and document it; and

3.1.6. where criminal offence information is processed, identify a lawful condition for processing that information and document it.

4. Rights of the Individual

4.1. The GDPR states that individuals have the following rights in respect of the processing of their Personal Information:

4.1.1. **The right to be informed**:

4.1.1.1. EA will keep individuals informed of its processing activities through its privacy which can be found on our website at www.eani.org.uk/privacy.

4.1.2. **The right of access**:

4.1.2.1. An individual may make a subject access request ("**SAR**") at any time to find out more about the Personal Information which EA holds on them. All SARs must be forwarded to the DPO using the contact details stated above.

4.1.2.2. EA is required to respond to a SAR within one month of receipt but this can be extended by up to two months in the case of complex and/or numerous requests and, in such cases, the individual will be informed of the need for such extension. The Authority does not charge a fee for the handling of a straightforward SAR.

4.1.3. **The right to rectification**:

4.1.3.1. If an individual informs EA that Personal Information held by EA is inaccurate or incomplete, the individual can request that it is rectified.

4.1.4. **The right to erasure**:

4.1.4.1. An individual is entitled to request that EA ceases to hold Personal Information it holds about them.

4.1.4.2. EA is required to comply with a request for erasure unless the Authority has reasonable grounds to refuse.

4.1.5. **The right to restrict processing**:

4.1.5.1. An individual is entitled to request that EA stops processing the Personal Information it holds about them in certain circumstances.

4.1.6. **The right to data portability:**

4.1.6.1. An individual has the right to receive a copy of their Personal Information and use it for other purposes.

4.1.7. **The right to object:**

4.1.7.1. An individual is entitled to object to EA's processing of their Personal Information.

4.1.8. **Rights in relation to automated decision making and profiling:**

4.1.8.1. An individual has the right to challenge any decision that is made about them on an automated basis (subject to certain exceptions).

4.1.8.2. EA is also required to comply with certain conditions if it uses Personal Information for profiling purposes.

5. Data Protection Officer

5.1. A Data Protection Officer (DPO) is appointed who will monitor adherence to this policy.

5.2. The DPO is required to have an appropriate level of knowledge of data protection and privacy matters within the EA.

6. Privacy by Design

6.1. EA has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process Personal Information will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

6.2. The data protection impact assessment will include:

6.2.1. Consideration of how Personal Information will be processed and for what purposes;

6.2.2. Assessment of whether the proposed processing of Personal Information is both necessary and proportionate to the purpose(s);

6.2.3. Assessment of the risks to individuals in processing the Personal Information;

6.3. What controls are necessary to address the identified risks and demonstrate compliance with legislation.

6.4. A data protection impact assessment is conducted:

6.4.1. On every business process periodically, at least once a year and more frequently where the amount and/or sensitivity of Personal Information processed, dictates so;

6.4.2. As part of the project calendar admission requirements checklist;

6.4.3. At every high-impact change, and/or at the request of the DPO.

7. Data Retention & Disposal

7.1. The longer that Personal Information is retained, the higher the likelihood is of accidental disclosure, loss, theft and/or information growing stale.

7.2. Any Personal Information kept by EA is managed in accordance with the Public Record Office (NI) Record Management Good Practice Guidance.

8. Data Breach

8.1. A data breach is any (potential) unintended loss of control over or loss of Personal Information within EA's environment. Preventing a data breach is the responsibility of all EA staff and its workforce.

8.2. Please refer to EA's Data Breach Management Procedure.

9. Third-Party Services and Subcontracting

9.1. EA may decide to contract with a third party for the collection, storage or processing of data, including Personal Information.

9.2. If EA decides to appoint a third party for the processing of Personal Information, this must be regulated in a written agreement in which the rights and duties of EA and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organisational security measures required in this Policy, and provide sufficient guarantees with respect to the protection of the personal rights and the exercise of those rights.

9.3. The subcontractor is contractually obligated to process Personal Information only within the scope of the contract and the directions issued by EA.

10. Complaints

10.1. Complaints will be dealt with in line with EA'scomplaints policy. You can find more information on this at http://www.eani.org.uk/about-us/comments-suggestions-and-complaints/.

10.2. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO's details are as follows:

The Information Commissioner's Office – Northern Ireland

3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk

11. Definitions

“consent”	is any freely given, specific and transparently, well-informed indication of the will of the individual, whereby the individual agrees that his or her Personal Information may be processed. Particular requirements about consent can arise from the respective national laws.
"Personal Information"	(sometimes known as “personal data”) means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly — in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
“processing”	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with Personal Information.
"Special Category Data"	(sometimes known as “sensitive personal data”) means Personal Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and the processing of data concerning health or sex life