DATA PROTECTION POLICY

Author: Danielle Faragher

Date of policy: September 2021

Ratified by Trust Board: September 2021

Review date: September 2022

CONTENTS

1. STATEMENT OF INTENT

1.1. At Education Impact Academy Trust (EIAT), we are committed to protecting the personal data of our staff, pupils, and visitors. We have a responsibility under the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) to obtain, record, hold, use, and store all personal data relating to an identifiable individual in a secure and confidential manner.

1.2. The Policy provides a framework within which we will ensure compliance with the requirements of the legislation and will underpin any operational procedures and activities connected with the processing of personal data.

1.3. This policy is in place to ensure all school employees, governors, volunteers, and contractors are aware of their responsibilities.

2. LEGAL FRAMEWORK

2.1. This policy has due regard to the following legislation:

- The General Data Protection Regulation
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The School Standards and Framework Act 1998

2.2. This policy also has due regard to guidance, including, but not limited to, the following:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

2.3. This policy will be viewed in conjunction with the following other Education Impact Academy Trust policies:

- Freedom of Information Policy

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual.
Special categories of personal data	Personal data which is considered to be more sensitive and therefore requires further safeguards: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data, where used for identification purposes (such as fingerprints, retina, and iris patterns) • Health – physical or mental • Sex life or sexual orientation • Criminal offences and procedures
Processing	Any operation or set of operations performed on personal data including collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual to whom the personal data relates.
Data controller	A person or organisation that determines the purposes and means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. DATA PROTECTION PRINCIPLES

4.1. In accordance with the requirements outlined in the UK GDPR, personal data will be:

4.2. Processed lawfully, fairly and in a transparent manner in relation to individuals.

4.3. Collected for specified, explicit and legitimate purposes and not 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.

4.4. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

4.5. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

4.6. 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

4.7. 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.

4.8. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. INDIVIDUALS RIGHTS

5.1. The UK GDPR provides the following rights for individuals:

5.2. The right to be informed - if your personal data is being used. Our privacy notice sets out the basis on which any personal data we collect or that is provided to us will be used.

5.3. The right of access - for copies of your personal information.

5.4. The right to rectification - to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

5.5. The right to erasure - to ask us to erase your personal information in certain circumstances.

5.6. The right to restriction of processing - to ask us to restrict the processing of your personal information in certain circumstances.

5.7. The right to object to processing - to object to the processing of your personal information in certain circumstances.

5.8. The right to data portability - to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

5.9. The right to prevent automated processing or ask us to explain decisions made by automatic processing - You have a right to prevent automated processing. Automated Processing is when decisions are made about you without people being involved.

6. ROLES AND RESPONSIBILITIES

6.1. This policy applies to all staff. You must be familiar with this policy and comply with its terms.

Governing Body and Trustees

6.2. The ultimate responsibility and accountability for compliance sits with governors and trustees. They have overall responsibility for ensuring compliance with all relevant data protection legislation and obligations.

6.3. They will ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the legislation.

Data Protection Officer

6.4. The Data Protection Officer (DPO) is Danielle Faragher who can be contacted by E-mail: Please contact us at: E-mail: dpo@educationimpact.org.uk: Tel: 0121 809 2489, Post: Education Impact Academy Trust Head Office, Wood End Road, Erdington B24 8BL.

6.5. The DPO is responsible for the following tasks:

- Producing and implementing data protection policies and procedures.
- Acting as the point of contact for and co-operating with the ICO.
- Investigating any suspected breaches and managing the response to an identified breach.
- Ensuring that any requests or complaints from individuals are dealt with promptly and appropriately.
- Monitoring compliance with relevant legislation and guidance.
- Informing and advising, any member of the workforce who processes personal data and any processor engaged by the Trust of their obligations under the legislation.
- Providing advice for the carrying out of a data protection impact assessment.
- Designing and coordinating data protection training and awareness programmes as appropriate.
- Monitoring data protection compliance, including carrying out audits.

Headteacher/ College Principal/ Nursery Manager

6.6. The Headteacher/ College Principal/ Nursery Manager will act as the representative of the data controller on a day-to-day basis.

6.7. They are responsible for the following tasks:

- Escalating any data protection concerns to the Data Protection Officer.
- Assisting the Data Protection Officer in investigating complaints and suspected breaches of data protection legislation or policy.
- Providing the Data Protection Officer with the necessary resources and access to personal data.

All Staff

6.8. All staff are responsible for:

- Collecting and using personal information in a fair and lawful manner with consideration for the rights of others.
- To only use personal data for the stated purpose unless explicit consent has been given by the data subject to use their information for a different purpose.
- To maintain the security of personal data.
- To accurately record personal data and ensure it is kept up to date.
- Undertaking relevant training.
- Reporting any enquiry, complaint, data subject access request or suspected breach to the Data Protection Officer.

Contractors, Agency Staff and Volunteers

6.9. All contractors, agency staff and volunteers are bound by the same code of behaviour and policies as school staff, including this policy.

6.10. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the breach and take remedial steps if necessary.
- maintain a register of breaches; and
- notify the Information Commissioner's Office if necessary.

7. PRIVACY BY DESIGN

7.1. We act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

7.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

7.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

7.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

7.5. The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented to address any risks to individuals
- Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

8. DATA BREACHES

8.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

8.2. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

8.3. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

8.4. If a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

8.5. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

8.6. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

9. DATA SECURITY

9.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access and will not be left unattended or in clear view anywhere with general access.

9.2. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

9.3. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

9.4. Staff will not use their personal laptops or computers for school purposes.

9.5. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g., keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

9.6. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are always supervised.

9.7. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a yearly basis or when there are changes to the facilities. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

10. CCTV AND PHOTOGRAPHY

10.1. We notify all pupils, staff, and visitors of the purpose for collecting CCTV images via notice boards, letters, and email.

10.2. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to keep staff, children, and visitors safe for the purposes of crime prevention and detection.

10.3. All CCTV footage will be kept for six months for security purposes; the IT Operations Manager is responsible for keeping the records secure and controlling access.

10.4. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

10.5. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the usage from the parent of the pupil.

11. REVIEW

11.1. This policy will be reviewed by the MAT Compliance/ Data Protection Officer on an annual basis, or sooner if there are any changes to relevant legislation.