Chief Executive Officer **MR JON HARRIS**

Data Protection Policy

Date adopted: March 2024

1. Statement of Intent

1.1. At Education Impact Academy Trust (EIAT), we are committed to protecting all personal data we hold. Our Trust processes personal data relating to parents and carers, pupils, staff, governors, visitors, and others, and therefore is a data controller. We are registered with the ICO and have paid our data protection fee to the ICO, as legally required

1.2. 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.

1.3. 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.

1.4. 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 all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK 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 2018) DfE (2023) 'Keeping children safe in education 2023'

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

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2023) 'Data protection in schools'

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

- CCTV Policy
- Data Retention Policy
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Safeguarding and Child Protection Policy

3. Data Protection Principles

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

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

3.3. 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.

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

3.5. 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.

3.6. 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.

3.7. 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.

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

4. Individuals Rights

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

4.2. 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.

4.3. The right of access - for copies of your personal information. Further info can be found at https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data

4.4. 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.

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

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

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

4.8. 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.

4.9. 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.

5. Roles and Responsibilities

Governing Body and Trustees

5.1. 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.

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

Senior Responsible Individual

5.3. The Data Protection and Digital Information Bill (DPDI), due to come into force in Spring 2024, stipulates that the Trust appoint a Senior Responsible Individual(s) (SRI), who is a named senior person(s) within the organisation. The Chief Executive Officer (Jon Harris) and Chief Finance and Operations Officer (Helena Mandleberg) will assume this role and will delegate day-to-day responsibilities to the Data Protection Officer.

Data Protection Officer

5.4. The Data Protection Officer (DPO) is the first point of contact for individuals, and for the ICO. Our DPO is Danielle Faragher who can be contacted by E-mail: dpo@educationimpact.org.uk: Tel: 0121 387 2005, Post: Education Impact Academy Trust Head Office, Wood End Road, Erdington B24 8BL.

5.5. The DPO is responsible for the following tasks:

- Producing and implementing data protection policies and procedures.
- 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 and conducting audits.

Executive Headteacher/ Nursery Manager

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

5.7. 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

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

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

5.10. 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.

6. Sharing of Personal Data

6.1. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. We share personal data with law enforcement and government bodies where we are legally required to do so.

6.2. We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

6.3. Data Protection legislation does not prevent or limit the sharing of information for the purposes of keeping children safe. We will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils.

6.4. We will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe

7. Data Breaches

7.1. 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.

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

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

7.4. 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.

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

7.6. 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

8. Data Security

8.1. 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.

8.2. 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.

8.3. 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.

8.4. Where possible, staff and governors will not use their personal laptops or computers for school purposes. All members of staff are provided with their own secure login and password if necessary.

8.5. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to the school are always supervised.

8.6. 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.

9. Data Retention

9.1. Personal data that is no longer needed will be disposed of securely in line with our retention policy. We overwrite or delete electronic files and securely shred paper-based records. We may also use a third party to safely dispose of records on the school's behalf.

10. Privacy by Design

10.1. We adopt a privacy by design approach and implement technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

10.2. 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.

10.3. 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.

10.4. 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.

11. CCTV

11.1. We notify all pupils, staff, and visitors of the use of surveillance and Closed-Circuit Television (CCTV) via CCTV signage, in line with our CCTV Policy.

11.2. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to keep staff, children, and visitors safe. CCTV is used for the following purposes:

- Out of hours surveillance of the site against intrusion or criminal activity.
- Prevention and detection of crime.
- To respond to serious incidents.
- Checking instances of physical damage to our sites.
- To support investigations into allegations.

11.3. All CCTV footage will be kept will be kept for a maximum of 30 days and then will be overwritten by the system. Any footage that is downloaded in terms of an event or investigation is securely stored and copies will be destroyed once they are no longer needed in line with our data retention policy.

12. Photography and Images

12.1. We use images and videos for a variety of purposes, including prospectuses, display boards, educational purposes, conferences, and the school website. We understand that parents may also wish to take videos or photos of their children participating in school events for personal use.

12.2. Staff members are provided with an iPad or tablet device with a camera to record and maintain pictorial evidence of the lessons, activities, and events related to their pupil's education. This processing is taking place in the performance of our duties as a public authority and is recorded as a 'public task' therefore consent is not required. These images and videos are used for educational purposes of recording pupil progress and evidence of learning.

12.3. Staff will not use their personal mobile phones, or any other personal device, to take images and videos of pupils.

12.4. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before using images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school productions.

12.5. Photos will not be used for marketing purposes unless the school has consent. The school will recognise that when images are posted on the school website or social media accounts that anyone may view the images. The school will therefore consider the suitability of images for use on the school's website.

12.6. We may use a professional photographer for official school photos and will inform parents beforehand. We always use a reputable company and do not allow the photographer unsupervised access with pupils.

APPENDIX 1: Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual.
Special categories of personal data	Personal data which is 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.