Chief Executive Officer **MR JON HARRIS**

EIAT DATA PROTECTION POLICY

Date adopted: March 2025

Next review: March 2026

Policy Author: Dannielle Knibbs

1. INTRODUCTION

1.1. Our Data Protection Policy lays out our approach to data protection. We recognise the importance of protecting the personal data we are entrusted with, and this policy sets out how we comply with relevant legislation.

1.2. If you have any queries about this Policy, please contact Dannielle Knibbs, Governance and Compliance Officer/Trust DPO, whose details can be found at the end of this policy.

1.3. This policy should be used in conjunction with the following EIAT policies.

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

2. RESPONSIBILITIES

2.1. This Policy applies to all staff, including temporary staff, governors, volunteers, and contractors, and anyone else working on our behalf.

2.2. All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to our Data Protection Officer.

2.3. All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it.

2.4. Our Data Protection Officer is responsible for advising us about our data protection obligations, dealing with breaches of this policy, including suspected breaches, identified risks, and monitoring compliance with this policy.

3. LEGISLATION

3.1. Relevant legislation includes:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;
- Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.
- Human Rights Act 1998
- Computer Misuse Act 1990, which covers unauthorised access to, and use of, computers and computer materials.

3.2. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.

3.3. Breaches of data protection legislation can result in significant monetary penalties and damage to reputation, as well as the risk of real harm to people whose data is handled in an unfair or unlawful way.

3.4. Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.

3.5. We follow the legal Data Protection Principles:

a) **Fair, lawful and transparent processing**: The reason for processing personal data must meet one of the legal conditions listed in Article 6 of the UK GDPR. Our data processing, including how and why we process data, is explained in our Privacy Notices

b) **Purpose limitations**: We only use the data we collect for the reasons explained in our privacy notice. If we need to use it for another reason, we will inform our data subjects of the new reason for processing before we do it.

c) **Data limitations**: We minimise the amount of data that we collect and process, keeping it to only what is necessary for the reasons we are collecting it. We should never collect or keep any personal data "just in case".

d) **Data accuracy**: We will always try to make sure the data we collect, and hold is accurate, and keep it up to date as appropriate.

e) **Data retention**: We only keep personal data for as long as is necessary for the reasons for which we are processing it, and we will be transparent with our data retention schedules. Any individual who purposefully retains data that they do not have authority for may be committing an offence under the DPA 2018 Section 170.

f) **Data security & integrity**: We use both technical and organisational security measures to protect data from unauthorised or unlawful processing, or from accidental loss, destruction or damage. Security measures should be appropriate to the level of risk involved in the data and the processing.

4. ARTIFICIAL INTELLIGENCE (AI)

4.1. We recognise that technology is rapidly evolving and are committed to remaining at the forefront of developments, adapting our ways of working as necessary.

4.2. AI is an integral part of the modern world and offers numerous opportunities for enhancing teaching, learning, and administrative processes, as well as potential risks, including to data protection principles.

4.3. We aim to foster a responsible and inclusive environment for the use of AI in education, upholding privacy, fairness, and transparency for the benefit of all involved.

5. DATA PROTECTION IMPACT ASSESSMENT (DPIA

5.1. A DPIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a DPIA should be used throughout the development and implementation of the school's project.

5.2. A DPIA will enable the school to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, as well as provide evidence of investigation into the suitability of any third parties who will be given access to data in the project.

5.3. DPIAs will be considered for all new projects that have been identified as processing personal data, at the earliest stages, to allow greater scope for influencing how the project will be implemented. Consistent use of DPIAs will increase the awareness of privacy and data protection issues within the trust and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

6. DATA BREACHES

6.1. If personal data we handle is lost, destroyed, altered, disclosed, accessed or put beyond use when it shouldn't be, this is a Personal Data Breach. A personal data breach can occur accidentally or intentionally, and can be caused by staff, by an external threat (including cyber incidents), or anyone else.

6.2. All breaches, or suspected breaches, of this policy will be reported **immediately** to the Executive Headteacher, or other senior leader in their absence, and the Data Protection Officer including if a breach is discovered outside of normal working hours.

6.3. Examples of Data Breaches

- Emails sent to wrong recipient
- Images of pupils uploaded without consent
- Device which stores personal data is lost e.g. iPad
- You access personal data for which you have no authorisation
- You share school personal data with people who have no authorisation

6.4. Where we *suspect* personal data has been subject to a breach, we will follow this procedure until we are sure that the personal data has or hasn't been breached.

6.5. Assess the risk (DPO)

The DPO will investigate appropriately and assess the risk, staff must communicate with the DPO all details of the breach. The DPO will consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely it is the harm will happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (that the data is about.)

The Executive Headteacher, IT Operations Manager and the DPO will take reasonable actions to contain the risks, and/or recover the data, if possible.

6.6. Notify the ICO of the breach (DPO).

Breaches that could cause a risk to people should be reported to the Information Commissioner's Office (the ICO – the UK's data protection regulator) and, in some cases, to the data subject(s) involved too.

Not all breaches will need to be reported. If the DPO decides not to report a breach to the ICO and/or the data subjects involved, the decision and reasons will be recorded.

If it *is* likely the breach will result in a risk to people's rights and freedoms, it must be reported to the ICO.

Reports to the ICO must be made within 72 hours of us becoming aware of the breach. Information can be provided to the ICO in stages, giving them the details as and when we find out more, but the first contact must be within 72 hours.

6.7. Notify the affected Data Subjects of the breach (DPO);

If the risk to data subjects is assessed as high, the breach must also be reported to everyone whose data is involved, to allow them to take any appropriate steps to protect themselves and so they are aware of anything that may happen.

We can choose to report to data subjects even if the risk is not high, if it would be better for us to tell them about the breach for other reasons, such as supporting transparent relations and trust. In many circumstances it will be preferable for data subjects to hear about a breach from us rather than from any other source.

6.8. Implement any necessary changes to prevent reoccurrence.

Clear actions will be taken to reduce the risk of something similar happening, including new or improved written procedures, refresher training, improved supervision, changes to processes, and communications to remind colleagues about risks, etc.

7. DATA RIGHTS

7.1. We process personal data in line with all legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing.
- Request access to their data that we hold
- Ask for inaccurate data to be rectified.
- Ask for data to be erased (sometimes known as the "right to be forgotten").
- Restrict processing of their data, in limited circumstances.
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing.
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person.
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects.
- Withdraw consent when we are relying on consent to process their data
- Make a complaint to the ICO or seek to enforce their rights through the courts.

7.2. The right to access applies to all pupils, parents, staff and anyone else that we hold personal data about. In some circumstances, for example with pupils, a parent or other person with authority may make the Subject Access Request on their behalf.

7.3. To exercise these rights or for further help and information about processing and our commitment to keeping data safe, please contact our Data Protection Officer, contact details can be found at the end of this policy.

8. SUBJECT ACCESS REQUESTS

8.1. All leaders are responsible for ensuring their team read and understand this procedure as they may receive a SAR on behalf of the school.

8.2. A SAR does not need to be in writing, it can be in any format, including a letter, email, text message, over social media, over the telephone, or face to face, and can be made to any representative of the school. **All SAR's received by school staff must be sent to the DPO without delay, school staff should never respond to a request themselves.**

8.3. A SAR does not need to be described as a subject access request to be a valid SAR. Any request for access to personal information from, or on behalf of, a data subject, should be treated as a SAR.

8.4. We must verify the identity of the person making the SAR, and if the SAR is being made on behalf of someone else, we must confirm they have authority to act on their behalf in exercising their rights.

8.5. A parent / person with parental responsibility does not automatically have the right to make a SAR on behalf of their child.

8.6. A child may exercise these rights on their own behalf if we believe they are competent to do so. Assessing competence is based on the age, maturity and level of understanding of the child. Each situation will be decided in collaboration with the professionals working with the child, but 12 years is regarded as a starting point. A child should not be considered competent if it is evident that he or she is acting against their own best interests or under pressure from a parent or other person with authority.

8.7. Where a SAR is received from a parent of a competent child, consent to process the request and release all/part of the information will be sought from the child.

8.8. SARs must be responded to within one month, school holidays and weekends are included in this time frame so **communication with the DPO is vital** so that the process is not delayed in any way. In the case of complex requests an extension of up to an extra two months can be applied, but the requestor must be informed of the extension within the first month.

8.9. Where the person's data is combined with another person's data, which does or could identify that other person (third party), that data may be redacted, or withheld if redaction would not fully prevent the other person being identified. Data can be disclosed that identifies the third party if that person has given their consent to disclose it, or it is judged to be reasonable to disclose the information without that person's consent.

8.10. Any written communication has the potential to be used in a SAR at any point, this includes emails. Emails must remain professional at all times.

8.11. Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided in a SAR to a data subject who has requested it, and has a right to receive it, may be committing an offence under the DPA 2018 Section 173.

9. FREEDOM OF INFORMATION REQUESTS

9.1. Requests for Environmental Information, for example, information about land development, pollution levels, energy production, and waste management will be dealt with under the Environmental Information Regulations 2004, all other requests will be dealt with under the Freedom of Information Act 2000

9.2. Where information is not published on our website, you may make a request by contacting the DPO in writing, by email or letter. We will, no later than 20 working days from receipt of the request:

1. Confirm or deny whether we hold information of the description specified in the request.
2. Provide the documentation, if we hold the requested information.

Except where:

a) We reasonably require further information to meet a request, have informed the requestor of this requirement, but have not been supplied with that further information.

b) The information is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.

c) A request for information is exempt under section 2 of the Freedom of Information Act 2000.

d) The cost of providing the information exceeds the statutorily imposed appropriate limit of £450

e) The request is vexatious.

f) The request is a repeated request from the same person made within 60 consecutive working days of the initial one

g) A fee notice was not honoured.

Where information is, or is thought to be, exempt, we will, within 20 working days, give notice to the requestor.

10. CONTACT DETAILS

Data Protection Officer	Dannielle Knibbs
DPO Email:	dpo@educationimpact.org.uk
DPO Address:	Education Impact Academy Trust, Head Office, Wood End Road, Erdington B24 8BL