Overarching Data Protection Policy

Data Protection: Our Approach

Document title	Overarching Data Protection Policy		
Owner	HR Operations Team HROT		
Version	1	Status	Draft
Last updated	21 Feb 2024	Last updated by	Lea Millinchip
Approved on	Pending	Effective from	Pending
Review on	TBC		
Purpose	This document outlines the framework which the Trust has in place to help ensure compliance with data protection law, including the UK GDPR and the Data Protection Act 2018 (DPA 2018).		

If you would like this information in another language or format, please speak to the Trust Human Resources.

Phone: 01543 622433

1.0 Purpose

1.1 This document outlines the framework which the Trust and its associated academies has in place to help ensure compliance with data protection law, including the UK GDPR and the Data Protection Act 2018 (**DPA 2018**).

1.2 Any references to colleagues include all colleagues working in the Trust (whether directly or indirectly), whether paid or unpaid, whatever their position, role, or responsibilities, which includes employees, Trustees, local academy committee members, contractors, agency colleagues, peripatetic colleagues, work experience / gap year / placement students and volunteers.

2.0 Roles, Responsibilities and Governance

2.1 The Trustees have appointed Lea Millinchip, Trust Compliance Officer, as the Data Protection Officer. The Data Protection Officer is responsible for advising on the Trust's compliance with data protection law. The Trustees have ensured that the Data Protection Officer has sufficient time and resources to fulfil their tasks.

2.2 The Data Protection Officer regularly reports to the Trust's Trustees who are responsible for the Trust's data protection compliance. Data protection is a standing item on the agenda at Trustees' meetings.

2.2 The Trust has appointed the Finance, Risk and Audit Committee with specific responsibility for data protection.

2.3 All colleagues have a role to play in our data protection compliance. Colleagues are encouraged to ask questions and raise concerns with the Data Protection Officer or their line manager. This allows us to regularly review and strengthen the data protection measures which we have in place.

3.0 Compliance measures

3.1 The Trust helps to ensure compliance with data protection law using the measures outlined at paragraphs 4.0 to 16.0 below.

4.0 Training

4.1 All colleagues receive data protection training as part of their induction and refresher training is provided annually. The training is online, and colleagues must pass a test to complete the training.

4.2 The training includes (but is not limited to) the practical application of the UK GDPR's principles in a school context, guidance on how to keep personal data secure and when colleagues should speak to the Data Protection Officer.

4.3 The Senior Leadership Team / Executive and Trustees receive additional training on an annual basis. This training has been specifically designed for their roles.

4.4 The Data Protection Officer attends external training annually which is appropriate to their role as the senior individual who leads on the Trust's data protection compliance.

Other teams and departments are given data protection training which is specific to their role or function as follows:

- Teaching colleagues – GDPR Awareness
- Business administration colleagues – GDPR for Education
- Principals – GDPR for Education
- All other colleagues - Basic GDPR

5.0 Policies and guidance

5.1 All colleagues at the Trust are required to comply with the following documents:

5.1.1 Data Protection Policy: Practical Guidance for Colleagues.

5.1.2 Information Security Policy; and

5.1.3 Guidance for Colleagues on the Use of Photographs and Videos.

5.2 The Data Protection Officer and Senior Leadership Team are responsible for implementing the:

5.2.1 Data Breach Policy and Procedure

5.2.2 Information and Records Retention Policy

5.2.3 CCTV Policy

5.2.4 Appropriate Policy Document for special category personal data.

6.0 Documentation

6.1 Documenting how we comply with data protection law is a key part of our compliance. In addition to the documents listed at section 5.0 above we:

6.2 Maintain a record of how we use personal data as required under Article 30 of the UK GDPR. The Data Protection Officer is responsible for maintaining this record.

- Document our lawful bases for using personal data through our privacy notices.
- Document our conditions for using special category personal data.
- Keep a record of our legitimate interests' assessments.
- Carry out risk assessments and when required a Data Protection Impact Assessment.
- Retain records of any consents obtained to use personal data
- Maintain a register of any data breaches. The Data Protection Officer is responsible for completing this. All colleagues understand that they must inform the Data Protection Officer of any suspected breach so that the register can be kept up to date.
- Record when colleagues' complete data protection training to ensure that all colleagues have received the appropriate level of training; and
- Maintain an Appropriate Policy Document regarding our processing of special category personal data and criminal offence data as required by the DPA 2018.

7.0 Privacy notices

7.1 The Trust has privacy notices which are published on the Trust's website.

7.2 We are mindful that some of our pupils are competent to exercise their own data protection rights. In light of this, we have developed a privacy notice for pupils which is age appropriate and addressed directly to the pupils.

7.3 In addition, the Trust explains how personal data will be used on a case-by-case basis as appropriate. For example, forms that are used to collect personal data will include a brief description of how and why it will be used, and cross refer to the applicable privacy notice.

8.0 Data protection by design and default

8.1 The Trust has built the data protection principles into its practices by implementing appropriate technical and organisation measures. This is known as data protection by design.

8.2 We also ensure that we only use the minimum amount of personal data to achieve our purposes - known as data protection by default.

8.3 More specifically we do the following:

- At the start of any new project, or new activity, which involves using personal data (e.g. working with a new external activity provider, implementing new software or hardware) the Data Protection Officer considers how we will comply with the data protection principles;
- We make it clear on any data collection forms what personal data must be provided and what is optional.
- We proactively consider data protection risks and adopt appropriate measures to protect personal data (e.g., encryption, physical security).
- Our external facing documents (e.g. privacy notices) are accessible and age appropriate.
- Before we share personal data externally, we check that we have a lawful basis and that the sharing is fair.
- We regularly review the measures which are in place to ensure that they are still appropriate.
- We have developed a culture where colleagues understand the importance of data protection; and
- If there has been a problem, or a "near miss", then we will look at what has happened to improve our practices, for example, by providing additional colleagues training and awareness.

9.0 The Trust has various internal written procedures in place to comply with our obligations under the UK GDPR. This includes in relation to:

- computer and network security
- the secure destruction of personal data - both electronic and paper copies
- individuals exercising their rights
- ensuring that we only use processors who comply with the UK GDPR; and
- physical security when the Trust site is used by external parties.

10.0 The Data Protection Officer determines whether a Data Protection Impact Assessment is required before the Trust begins any new type of processing activity. For example, before the Trust introduces new software to store pupil records.

11.0 Individuals' rights

11.1 We are committed to allowing individuals to exercise their rights under the UK GDPR. These rights are as follows:

- Right of access (i.e., making a subject access request);
- Right to rectification.

- Right to erasure.
- Right to restriction.
- Right to data portability.
- Right to object; and
- Rights in relation to automated decision-making and profiling.

11.2 Colleagues are trained to recognise when an individual is exercising a right under the UK GDPR and to pass this immediately to the Data Protection Officer.

11.3 The Trust keeps a log of all requests to exercise rights with the applicable deadline for our response. This log is maintained by the Data Protection Officer.

11.4 To ensure that we meet our obligations the Data Protection Officer co-ordinates our response to all requests. The Data Protection Officer has detailed knowledge of how to respond to individuals' rights and has received external training. The Data Protection Officer will involve other members of colleagues, as appropriate, in formulating the Trust's response.

11.5 Consideration is given to at least the following issues when responding to rights requests:

- The importance of responding within the statutory timeframe, usually one calendar month (but this can be extended by up to two months for complex requests).
- Whether a pupil's authorisation should be sought before responding to their parent or guardian.
- Whether further engagement with the requester is needed, e.g. to ask for ID or to seek clarification of their request;
- The exemptions under the DPA 2018.
- The provision of supplementary information (e.g., sources and purposes) under a subject access request.
- Whether the request can be refused, or a reasonable fee charged, because it is manifestly unfounded or excessive; and
- How to securely send our response to the requester.

12.0 Information security

12.1 The Trust has put in place technical and organisational measures to ensure the confidentiality, availability and integrity of personal data. The Data Protection Officer is responsible for determining the appropriate organisational measures, for example, colleagues training and guidance.

12.2 The Executive Team leads on the technical side of our information security, for example, network security. The Trust follows guidance from the National Cyber Security Centre and keeps up to date with the latest cyber security news and alerts.

12.2 The Trust has implemented an Information Security Policy for colleagues.

12.3 We appreciate that prompt action is vital when handling information security incidents. Colleagues are trained to report any suspicions or concerns regarding potential personal data breaches to the Data Protection Officer immediately.

12.4 The Data Protection Officer will carry out an initial investigation and determine if the incident constitutes a personal data breach. If so, the procedure outlined in the Data Breach Policy and Procedure will be followed.

13.0 Processors

13.1 The Trust has procedures in place to check that the organisations acting as our processors are complying with the UK GDPR. The Data Protection Officer and Director of Operations are responsible for implementing these procedures.

13.2 The Trust has contracts in place with our processors which include the specific terms required by the UK GDPR. Legal advice is sought as required regarding these contracts.

13.3 Colleagues are trained to speak to the Data Protection Officer if they need to share information with an organisation which may act as the Trust's processor so that the Data Protection Officer can check that the appropriate measures are in place.

14.0 International transfers

14.1 The Trust maintains a record of when it transfers personal data outside of the UK and what adequacy decision, safeguard or derogation is relied on under the UK GDPR. The Data Protection Officer is responsible for maintaining this record.

14.2 Colleagues are trained to speak to the Data Protection Officer before transferring personal data outside of the UK.

15.0 Data Protection Fee

15.1 The Trust has procedures in place to ensure that the data protection fee is paid to the Information Commissioner's Office for all controllers connected to the Trust.

15.2 The Finance Director is responsible for ensuring the fee is paid on time.

16.0 Monitoring and review

16.1 The Data Protection Officer will ensure that the content and implementation of the procedures set out in this policy are reviewed regularly.

16.2 Any personal data breaches at the Trust will be followed by a review of the relevant procedures by the Data Protection Officer and a report made to the trustees.