Data Protection Policy

Document Detail	
Policy Reference Number:	62
Category:	Pupil Related
Authorised By:	Trust Board
Status:	Approved
Chair of Trust Board Signature	
Date Approved:	December 18
Issue Date:	December 18
Next Review Date:	December 20

Contents

Introduction

The Inclusive Multi Academy Trust regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose and vital for maintaining confidence between employees, pupils and others whom we process data about, on behalf of and ourselves.

Policy Statement

This Data Protection Policy explains how the Trust will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) (the Legislation) which cover data security and confidentiality of personal and sensitive personal data. (A list of important defined terms in the GDPR can be found on the back pages of this policy).

The Trust will

- fully implement all aspects of the legislation.
- ensure all employees and others handling personal data are aware of their obligations and rights under the legislation.
- implement adequate and appropriate physical, technical and organisational measures to ensure the security of all data contained in or handled by those systems.

The main focus of this policy is to provide guidance about the protection, sharing and disclosure of employee and client data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or sensitive (to be called "Special Category" in the GDPR) data on behalf of the Trust.

Registration with the Information Commissioner

GDPR requires data controllers (to register with the Information Commissioner (ICO) the categories of personal data they hold, and what they do with it. The Trust is registered with the ICO. The Trust is a "data controller" when it decides how to use personal data. It is a "data processor" when it is directed by a third party as to how to use personal data. Further to the GDPR both data controllers and data processors have legal obligations to safeguard personal data and are both liable if there is a breach.

Definitions of Personal Data and Sensitive Personal Data

Personal data is any personally identifiable information, so this includes:

- employee data
- client data
- any other personal data processed by the Trust

Examples of personal data which the Trust processes include:

- Names, addresses, emails, phone numbers and other contact information;
- Financial information;
- National insurance numbers and payroll data;

- CCTV images and photographs, video and audio recordings.

Certain types of data are identified as sensitive or "special category" and attract additional legal protection. Sensitive personal data is any data that could identify a person together with information about their:

- racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexual life;
- Commission or alleged commission of any offence;
- Information about any proceedings for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of a court in such proceedings.
  .

Data Protection Principles

We must all comply with the six Data Protection principles that lie at the heart of the Legislation. The Trust fully endorses and abides by the data protection principles. Specifically, the six principles require that data is:

- **Principle 1:** Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').
- **Principle 2:** 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 ('purpose limitation').
- **Principle 3:** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- **Principle 4:** 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 ('accuracy').
- **Principle 5:** 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 ('storage limitation').
- **Principle 6:** 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 ('integrity and confidentiality').

Personal data and sensitive personal data must not be used other than for specific purposes. The data subject should always know that their data is being processed and the purpose. This information is provided in our Privacy Policies. When that data is sensitive, for example health information, consent is required before the data can be processed by the Trust.

All data collected from young people under the age of 16 (unless there are concerns about mental capacity in which case this should be extended), is not classed as sensitive personal data but should be treated as sensitive personal data.

A record incorporating personal data can be in computerised and/or manual form. It may include such documentation as:

- Manually stored paper data e.g. employee records.
- Hand written notes.
- Letters to and from the Trust.
- Electronic records.
- Printouts.
- Photographs.
- Videos and tape recordings.

Backup data (i.e. archived data or disaster recovery records) is also subject to the legislation. A search in backup data should only be conducted if specifically asked for by the data subject.

Rights of Individuals

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object to processing.
- Rights in relation to automated decision making and profiling.

The Right of Access

The legislation gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled, i.e. hand written records, electronic and manual records held in a structured file, subject to certain exemptions. This is called a Subject Access Request. The legislation treats personnel data relating to employees and clients alike.

Retention Periods

We store data in accordance with the criteria set out in our Data Records Management and Retention Policy.

Practical Implications

Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller. Therefore, the Trust will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a lawful basis for using personal data.
- Ensure that the use of the data is fair and will meet one of the specified conditions.
- Only process sensitive personal data where the Trust has obtained the individual's explicit consent; unless an exemption applies.
- Only process sensitive personal data, if it is absolutely necessary for the Trust to use it.
- Explain to individuals, at the time their personal data is collected, how that information will be used (within our Privacy Policies).
- Only obtain and use personal data for those purposes which are known to the individual.
- Only process personal data for the purpose for which it was given. If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is relevant to the Trust.
- Keep personal data accurate and up to date.
- Only keep personal data for as long as is necessary.
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving bulk information with exception of core administrative emails such as renewals. The Trust will always suppress the details of individuals who have opted out of receiving information (e.g. marketing).
- Will always give an option to "opt in" when consent is needed to process personal data unless there is a statutory/ legal exemption.
- Take appropriate technical and organisational security measures to safeguard personal data.

In addition, the Trust will ensure that:

- It appoints a Data Protection Officer with specific responsibility for Data Protection
- Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are promptly and courteously dealt with.
- Methods of handling personal data and sensitive personal data are clearly described in polices and guidance.
- A review and audit of data protection arrangements is undertaken annually by the Data Protection Officer
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Data Protection Officer.
- Formal written data processing agreements are in place before any personal data and sensitive personal data is transferred to a third party.

Roles and Responsibilities

Maintaining confidentiality and adhering to Data Protection Legislation applies to everyone at the Trust. The Trust will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees/Volunteers, Governors and Trustees will receive training and sign this policy as part of their induction.

All employees, volunteers and sub-contractors/associates have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data
- Obtain and process personal data and sensitive personal data only for specified purposes
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work
- Record data correctly in both manual and electronic records
- Ensure any personal data and sensitive personal data held is kept secure
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party
- Ensure personal data and sensitive personal data is sent securely

All Line Managers are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled, and that the data is only used for the intended purposes(s)
- Providing clear instructions to their teams about data protection requirements and measures;
- Ensuring personal and sensitive personal data is only held for the purpose intended;
- Ensuring personal and sensitive personal data is not communicated or shared for non authorised purposes; and
- Ensuring personal and sensitive personal data is encrypted when transmitted or appropriate security measures are taken to protect when in transit or storage.

Our Data Protection Officer is Andrew Chappell. Responsibilities include:

- Ensuring compliance with legislation principles;
- Providing guidance and advice to employees in relation to compliance with legislative requirements
- Auditing data protection arrangements continually
- Reporting on any breaches of Data Protection Legislation
- In the Data Protection Officer's absence, advice and general information can be found at http://www.ico.gov.uk/
- Ensuring those handling personal data are aware of their obligations by producing relevant policy, auditing the arrangements and ensuring relevant people receive training.

The Headteacher is responsible for Data Protection within their school. The Trust relies on each of its employees and sub-contractors/associates to help in ensuring secure systems are in place to protect personal data.

The Information Commissioner Office (ICO) – The Information Commissioner's Office is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with the Legislation may lead to an investigation by the ICO which could result in serious financial or other consequences for te Trust.

Breach of Policy

In the event that we fail to comply with the Legislation, an individual can complain to the DPO and/or ICO. We respectfully request that you notify the DPO in any event.

Dealing with a Data Breach
Data Breach Process

Although the Trust takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the Trust

However the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified the breach has occurred must notify the Trusts DPO, Andrew Chappell. A record of the breach should be created using the following templates:
    a. Data Breach Incident Form (Appendix A)
    b. Data Breach Log (Appendix B)
    c. Evidence Log (Appendix C)

2. **Containment:** DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. **Assess the risks:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form (Appendix C):

    a. What type of data is involved
    b. How sensitive is it?
    c. If data has been lost/stolen, are there any protections in place such as encryption?
    d. What has happened to the data?
    e. What could the data tell a third party about the individual?
    f. How many individuals data have been affected by the breach?
    g. Whose data has been breached?
    h. What harm can come to those individuals?
    i. Are there wider consequences to consider such as reputational loss?

5. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

    The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the Headteacher.

7. **Evaluation:** The DPO should assess whether any changes need to be made to the Trust processes and procedures to ensure that a similar breach does not occur.

Glossary of Terms

Consent
Clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic) statement.

Data Subject
Means an individual who is the subject of personal data or sensitive personal data. This includes an employee, client or other identifiable individual.

Data Controller
Means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed. The data controller is the Trust for employee data.

Data Processor
In relation to personal data or sensitive personal data, means any person who processes data

Third Party
In relation to personal data or sensitive personal data, means a natural or legal person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the police or HMRC.

Personal Data
Any information relating to an identified or identifiable natural person ('data subject'): an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Processing
Means recording or holding data or carrying out any operations on that data; including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it. Essentially if you have it, you are processing it.

Data Breach
Is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data transmitted, stored or otherwise processed.

Subject Access Request
This is a written, signed request (which includes emails and other written formats) from an individual to see data held on them. The Data Controller must provide all such information in a readable form within 30 days of receipt of the request.

Appendix A

Data Breach Incident Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:

What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	
Whose data has been breached:	
What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss:	

Part C: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No

	If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	

Appendix B

Data Breach Log

Date Reported:	Notified By:	Reported To:	Description of Breach:	Notification to ICO:	Notification to Individual(s)	Further Actions to be taken:	Reviewed by:
				Yes/No	Yes/No		
				Yes/No	Yes/No		
				Yes/No	Yes/No		

Appendix C

Data Breach: Evidence Log

Date:	Description of Evidence:	Details of where evidence is stored/located:	Member of staff who collected data: