Eastern Multi-Academy Trust
Empower - Motivate - Aspire - Transform

Policy	**Data Protection Policy**
Author	Alan Evans
Date of Approval	July 2014
Approved by	Board
Review date	July 2016

This document is a statement of the aims and principles of the Trust, for ensuring the appropriate handling of personal and sensitive information relating to staff, pupils, parents and governors.

This policy takes due note of the information and guidance published by the Information Commissioners Office (http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)

It is the responsibility of the Trust to ensure registration with the ICO is undertaken.

1. Introduction

1.1 All academies in the Trust need to keep certain information about employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

1.2 To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Trust and its academies must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

1.3 In summary these principles state that personal data shall:

Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

Be adequate, relevant and not excessive for that purpose.

Be accurate and kept up to date.

Not be kept for longer than is necessary for that purpose.

Be processed in accordance with the data subject's rights.

Be kept safe from unauthorised access, accidental loss or destruction.

1.4 All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Trust has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the Trust and its Academies from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2. The Data Controller and the Designated Data Controllers

2.1 The Eastern Multi-Academy Trust as the corporate body is the Data Controller under the 1998 Act, and the Directors are therefore ultimately responsible for implementation. The Trust Finance Director is the Designated Data Controller for the Trust. However, the Designated Data Controllers in each Academy will deal with day to day matters.

2.2 Each academy has two Designated Data Controllers. They are the Principal and a nominated senior member of support staff.

2.3 Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

3. Responsibilities of Staff

3.1 All staff are responsible for:

- Checking that any information that they provide to the Trust in connection with their employment is accurate and up to date.
- Informing the Trust of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Trust cannot be held responsible for any errors unless the staff member has informed the Trust of such changes.
- Handling all personal data (e.g. pupil attainment data) with reference to this policy, the academy's confidentiality policy and the guidelines in the staff handbook.

4. Data Security

4.1 All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

4.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

4.3 Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or

- If it is computerised, be encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a usb memory stick or other removable storage media, that media must itself be encrypted/password protected and/or kept in a locked filing cabinet, drawer, or safe.

4.4 All staff should be aware of the risks involved when working remotely as regards data security and take appropriate action:
- Take steps to avoid theft and do not leave items unattended
- Ensure that unauthorised people cannot view documents or data

5. Rights to Access Information

5.1 All staff, parents and other users are entitled to:
- Know what information the Trust / academy holds and processes about them and / or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the Trust / Academy is doing to comply with its obligations under the 1998 Act.

5.2 The Trust / Academy will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Trust / Academy holds and processes about them, and the reasons for which they are processed.

5.3 All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Designated Data Controller.

5.4 The Trust / Academy may make a charge on each occasion that access is requested, although the Trust / Academy has discretion to waive this.

5.5 The Trust / Academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

6. Retention of Data

6.1 The Trust / Academy has a duty to retain some staff and pupil personal data for a period of time following their departure from the Trust / Academy, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time. Some examples are noted below (Source: A model policy and guide for schools June 2012):

- School records for a child should be kept for 7 years after the child leaves the academy, or until the child reaches 25 years of age (whichever is greater) and examination records the same.

- Records of applications and admissions to the academy will be retained for a minimum period of ten years, as required by DfE
  Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc.) these records should be retained as set out by HR.

  Interview records, CV's and application forms for unsuccessful applicants are kept for 6 months.
  All formal complaints made to Principals or Governors will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.

7. Complaints

7.1 Complaints will be dealt with in accordance with the Trust's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

8. Monitoring and Evaluation

8.1 This policy will be reviewed every 2 years, or if there are changes to relevant legislation.