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

Policy and Procedure:	**Data Protection Policy**
Version:	v 1.3
Author:	Alan Evans
Approved by:	Audit Committee
Date of Approval:	June 2019
Amended / Updated:	October 2019
Review date:	June 2022

Introduction

This document is a statement of the aims and principles of the Trust for ensuring the appropriate handling of personal and sensitive data relating to staff, pupils, parents, Members, Trustees and Academy Council members.

This policy takes due note of the information and guidance published by the Information Commissioners Office ICO and the Department for Education DfE.

Information and Communication Technology (ICT) is increasingly used to support the delivery of the Trust's services and management processes. Hardware and software that make up ICT equipment, the data they process and store, and the information flows that they support are therefore vital resources.

The large quantities of personal and confidential information stored electronically or in paper format means that the greatest care should be taken to ensure security of the Trust's data systems.

Section A - Who does this policy apply to?

These policies, framework and any references to 'the Trust' or 'users' refer to, but are not limited to, Members, Trustees, Academy Council members, all Trust staff, agency workers, contractors, third parties and temporary staff such as work placements.

Responsibilities of the Chief Executive and Principals

The Chief Executive and Principals will support this policy by:

- Promoting the IT Security and GDPR framework within the Trust and Academies, and ensuring that the supporting Polices are circulated to all personnel.
- Ensuring that all members of staff understand the legal risk and security implications of improper use of Trust and Academy ICT facilities.
- Emphasise the obligations placed on all members of staff for their own compliance to information and data security for the Trust.
- Promoting best practice in terms of security and data protection
- Defining within the Senior Leadership Team the acceptable level of personal use for Trust and personally owned hardware such as mobile phones and facilities such as personal email accounts etc.

The Chief Executive and Principal will ensure that the ICT facilities are configured and operated appropriately to protect the information held within or accessed by them.

KEY MESSAGE
All members of staff must be aware of their obligations under this policy and take reasonable action to ensure on-going compliance. It is the responsibility of the Chief Executive and Principals to ensure this is in place. It is the responsibility of users to ensure that they keep up to date with the latest requirements and adherence to the supporting policies and procedures.

Section B – Scope & General Principles

All academies in the Trust need to keep certain information about employees, pupils and other users to allow, for example, performance & achievement monitoring, and health & safety. It is essential that this be handled appropriately.

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 appropriate legislation and Data Protection Principles which are set out in the 2018 General Data Protection Regulations (GDPR); Data Protection Act 2018 (DPA2018); Freedom of information Act 2000 (FoIA) and the Public Interest and Disclosure Act 1998 (PIDA).

The regulatory body responsible for the Trust's adherence to such legislation in the UK is the Information Commissioner's Office (ICO), which is a non-departmental public body reporting directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport.

It is the responsibility of the Trust to ensure registration with the ICO is undertaken for the Trust and its academies.

In summary GDPR 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.

All members of 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 as part of a larger GDPR framework.

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 this policy or additional guidance can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

Eastern Multi-Academy Trust as the corporate body is the Data Controller under the Regulations and the Trustees are therefore ultimately responsible for implementation and ensuring that all academies comply with all relevant data protection obligations.

The Trust has appointed an external Data Protection Officer (DPO). The DPO is responsible for overseeing the implementation of this policy, monitoring compliance and developing relevant guidance and policies where applicable.

The DPO may be contacted by email dpo@brigantia.com
As the DPO service is outsourced, staff may also contact the Deputy Chief Executive in regards to data protection matters alan.evans@eastern-mat.co.uk

Within each academy the Principal is responsible for the management for data, with operational guidance provided by the Trust Deputy Chief Executive and the Data Protection Officer (DPO).

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself/herself or their child is encouraged to raise the matter with the Principal, senior leadership team or the DPO.

Responsibilities of Staff

All members of 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 provided on the handling of data.
- Staff should contact their Principal, Chief Executive or the DPO is they have any concerns that this policy is not being followed or if guidance is needed on the use or sharing of personal data

KEY MESSAGE
Remember, IT security and data protection are the responsibility of all members of staff.

Data Security

All members of staff are responsible for ensuring that personal data that they hold is kept securely and that it is not disclosed either orally, in writing, online or by any other means, accidentally or otherwise, to any unauthorised third party.

All sensitive information will be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident. Broadly, this means:

- Anything of a personal nature that is not a matter of public record about students, applicants, staff members or trust members.

- Sensitive organisational information that could be used to damage the trust or threaten the security of the trust's business, property or buildings.

- Commercially sensitive information, tenders and quotations for services and works.

For the avoidance of doubt, handling of sensitive information includes; paperwork, telephone calls, emails and electronic documents wherever they may be stored.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe;
- If it is computerised, be encrypted **and** password protected, both on a local hard drive and on a network drive that is regularly backed up;

- If a copy is kept on a USB memory stick or other removable storage media, that media must itself be encrypted **and** password protected, and kept in a locked filing cabinet, drawer, or safe;
- Take steps to avoid theft and do not leave items unattended;
- Ensure that unauthorised people cannot view documents or data.

All staff should be aware of the risks involved when working remotely as regards data security and take appropriate action.

Rights to Access Information

As part of the changes introduced in GDPR, more emphasis has been placed on the rights of the data subject than ever before. All staff, parents and other users (all data subjects) have a right under the Data Protection Act 2018 to access personal data being kept about them or their child either on computer or in certain files.

They are entitled to:

- Know what information the Trust / academy holds about them and / or their child;
- 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 Data Protection Act 2018.

KEY MESSAGE

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you store or process personal data:

(a) Consent:	the individual has given clear consent for you to process their personal data for the specific purpose that you using it for.
(b) Contract:	the processing is necessary for fulfilment of a contract with the data subject, or because the data subject have asked for specific steps to be taken before entering into a contract.
(c) Legal obligation:	the processing is necessary so as to comply with the law (NOT including contractual obligations).
(d) Vital interests:	the processing is necessary to protect someone's life.
(e) Public task:	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The Trust / Academy will, upon request, provide 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.

This process is known as a Data Subject Access Request and can be best achieved by the completion of the Data Subject Access Request (DSAR) form: although completion of this form is not a requirement for starting a Data Subject Access Request, it is usually helpful and may increase the speed with which the request can be processed.

Any person who wishes to exercise this right should make a request with a member of staff who in turn should refer it to the Principal, senior leadership team or the DPO.

The Trust / Academy aims to comply with Subject Access Requests for personal information and Freedom of information requests as quickly as possible. A Data Subject Access Request will usually be dealt with within one month, while a Freedom of Information request will be dealt with within 20 school days or sixty days (whichever is less).

Members of staff will generally have access to all information that they need to fulfil their role. Members of staff are under a duty to respect the confidentiality of all personal information held by the Trust / Academy.

The Trust / Academy is responsible for ensuring that suitable data sharing agreements are agreed and recorded with appropriate third-party organisations prior to the sharing of data. This is necessary to maintain the data subjects' rights under governing legislation.

The Trust / Academy also reserves the right to regularly audit new and pre-existing data sharing agreements to ensure these remain accurate and relevant, updating them where necessary.

Disclosure

Disclosure of personal information outside the Trust will only be made with the written consent of the individual concerned, except:

- To comply with the Law or a Court Order.
- Where there is a clear health or safety risk or evidence of fraud.
- Where there is a Safeguarding risk or concern, or it is necessary to protect life.
- To be shared with a third party, contractors or other agents providing services on the Trust's behalf, subject to an appropriate data sharing agreement. The third party, contractors or other agents will be subject to the same level of confidentiality and regulatory compliance as the Trust / Academy.

- Anonymised for bona fide statistical or research purposes, provided it is not possible to identify the individuals to whom the information relates.

KEY MESSAGE

Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.

The data protection legislation, including GDPR, does **not** prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support that they need.

Information can be shared without consent if the process of gaining consent would place a child at risk.

As with all data sharing, appropriate organisational data sharing agreements and technical safeguards (encrypted data) should remain in place.

In all cases, follow your academy's safeguarding procedures. In the event of there being any perceived conflict between safeguarding procedures and data protection procedures, the safeguarding procedures should be deemed to be the governing procedures.

Retention of Data

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. For full details, please refer to the Trust Data Retention Policy which is based on the DfE Retention Timetable document.

Disposal

Subject to the timescales set out in the Trust Data Retention Schedule, all personal information (including computer printouts of personal and sensitive data, personally Identifiable Information (PII) and other information relating to data subjects, both former and current) will be deleted, shredded or destroyed when no longer required.

Please consult the Data Retention Policy for further guidance on obligations and processes under the Data Protection Act 2018.

Data Loss or Data at Risk

Data loss is where confidential data, potentially subject to the Data Protection Act 2018, has been released beyond the normal control environment, either by accident, not following laid down procedures, theft or other means.

Data at risk is where confidential data has not been released beyond the normal control environment but could be exposed or at risk due to a lack of appropriate control measures or failure of existing systems and processes.

Any individual within the scope of this policy who identifies what they believe to be confidential data at risk, should inform the Principal, senior leadership team or DPO

In the event that data loss is identified, report this immediately to the Principal, senior leadership team or the DPO where further guidance will be provided.

A number of steps must be completed as detailed within the Data Breach Response and Notification Procedure including recording the concern/loss/impact on the Trust's Data Protection register.

Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

We use CCTV in various academies across the Trust to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Academy Principal.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Primary academies:

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Secondary academies:

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data protection by design and default

We will endeavour to put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly updating members of staff and Trustees on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

Complaints

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's Office (the statutory regulator).

Monitoring and Evaluation

This policy will be reviewed every 3 years, or sooner if there are changes to relevant legislation.

Section C - Data Protection Policy – supporting policies and procedures

This Data Protection Policy is a statement of the aims and principles of the Trust for ensuring the appropriate handling of personal and sensitive data relating to staff, pupils, parents, Members, Trustees and Academy Council members.

It is supported by a range of policies and procedures. This list is not exhaustive and may be added to as necessary

Policies

- Acceptable Use of IT – for staff
- ICT for students
- E-safety policy
- Data Retention Policy and Schedule
- Freedom of Information Policy and Model Publication Scheme
- CCTV and Surveillance Policy

Procedures

- Subject Access Request procedures
- Data Security Breach procedures
- Data Security Breach Report form

Notices

- Privacy Notice – Staff
- Privacy Notice – Pupils
- Privacy Notice – Trustees and Members

Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as 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 whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the 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.