Data Protection Policy

Date Policy Reviewed / Developed:	**March 2019**	
Title:	**Data Protection Policy**	
Summary of Policy:	**This policy reflects the commitment of the Esteem Multi-Academy Trust (EMAT) to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018.**	
Policy Author:	John Walker - DPO	
Policy Agreed By: Trust Board/CEO/Committee	Agreed By: Julian Scholefield - CEO Rebecca Bage- Governance Officer	Date: March 2019
Policy Enquiry Contact details:	Rebecca Bage rbage@esteemmat.co.uk	
Additional documents/references related to this policy:	Finance Handbook Data Protection Act 2018	
Academy Specific / MAT wide	MAT wide policy	
Review Period:	3 years	
Date Review Due:	March 2022	

DATA PROTECTION POLICY MARCH 2019

Approved: 29/03/19
Version 1.0

Data Protection Policy –

Esteem Multi-Academy Trust

Introduction

The Esteem Multi-Academy Trust (EMAT) is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018.

The Trust gathers and processes personal information about its staff, students, and other individuals to comply with obligations as a charitable company limited by guarantee that is responsible for academies. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Any breach of the Data Protection Act 2018 or this Trust Data Protection Policy is considered to be an offence, and in that event relevant disciplinary procedures will apply. The contents of this policy are applicable to employees, trustees and governors, other agencies and providers working with the Trust, and who have access to personal information.

EMAT is the Data Controller and is responsible for setting the overarching policy and standards for Data Protection. The trust see compliance with these obligations as the best method to ensure that personal information is dealt with lawfully and securely and in accordance with the GDPR and other related legislation.

It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. It applies to all data held in schools as part of the multi-academy trust, though the responsibility for managing data rest with each school, and they school shall provide a Data Protection Policy and suitable Privacy Notices.

All schools within the trust process personal information about staff, pupils, parents and other individuals who come into contact with each academy as part of the usual day to day business of a school. The schools are required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other legislation.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 3 years.

Each academy within the trust will have the relevant polices and procedures published on their own website.

Background to the Data Protection Act 2018

The Data Protection Act 2018 brings into UK law the requirements of General Data Protection Regulations ("the GDPR") which is a European Directive.

The GDPR (and hence the Data Protection Act 2018) exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The GDPR exists to protect individual rights in an increasingly digital world.

What is Data?

Data is any information that relates to a living person which identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include personal opinions. The individual defined by the data is called the Data Subject.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

The Trust often collects sensitive data for the Department for Education and Local Authority requirements. Of course, student data may contain information about safeguarding, special education or health needs. Information about other family members may also be held.

Every Academy within the Trust must publish a Data Protection Policy and suitable Privacy Notices on their website that reflect the overarching principles set out by the Trust.

What are the key principles of the GDPR?

Lawfulness, transparency and fairness:
The Trust must have a legitimate reason to hold the data, this is explained in the Privacy Notices. Consent is often sought to use data about a student for a particular purpose, however there are other grounds for collecting and processing data to ensure that we meet out legal obligations.

Collect data for a specific purpose and use it for that purpose:
Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection:
The Trust recognises that, as an organisation, we must collect the minimum amount of data needed for a particular task or reason.

Accuracy:
Data collected should be accurate, and steps should be taken to check and confirm accuracy. The frequency of the checks depends on who or what data we are collecting and processing in the Academies.

The Trust recognises and supports the rights of Data Subjects to object if they feel that the information held is inaccurate, should no longer be held by the Data Controller or should not be held by the Data Controller in any event a dispute resolution process and complaint process can be accessed.

Retention:
The Trust has a retention policy that sets out how long records are kept.

Security:
Ensuring that suitable processes and procedures are in place is a requirement for each Academy and the Trust. This includes paper files, electronic records or other information.

Data Subjects' rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected.

There are other rights that relate to automated decision making and data portability that are not directly relevant to Academies of Academy Trusts.

Data Subject's rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. The Trust also has legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

Subject Access Requests

Individuals can ask for copies of information that is held about them or a student for whom they have parental responsibility by way of a Subject Access Request. This Subject Access Request process is set out separately and should be made directly to the relevant academy.

Information requested must be provided within a month but this can be extended if, for example, the Academy was closed for holidays. The maximum extension permitted is two months.

Information provided by a third party is not usually released without their consent.

Information will be supplied in an electronic form.

Who is a 'Data Controller'?

The Trust is the Data Controller (i.e. the Board of Directors). They have ultimate responsibility for how Trust manages data. They delegate this to Data Processors to act on their behalf.

Who is a 'Data Processor'?

A Data Processor is any person that uses, collects, accesses or amends the data that the Data Controller has collected or authorised to be collected. It can be a member of staff, a third-party company/service provider, a governor, a contractor or a temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful with the data as the Data Controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

The Trust must have a reason to process the data about an individual. Privacy notices set out how we use data. The GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it must fall within one of those conditions.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Data sharing

Data sharing is only carried out within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded on a case by case basis.

Retention

Each academy within the Trust gas a retention policy, some information is governed by statutory and regulatory requirements, others are determined by local practice and practicality.

Breaches & non-compliance

If there is a non-compliance with this policy or the processes it sets out, or there is a breach as described within the GDPR and Data protection Act 2018 then the Trust will be notified as soon as the breach is discovered.

If there is a data breach there is a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible. Each academy will have a breach management action plan

Protecting data and maintaining data subjects' rights is the purpose of this policy and its associated procedures.

Consent

The Trust will seek consent from staff, volunteers, students, parents and carers to collect and process their data. The reasons for requesting the data (and how it will be used) will be made clear.

There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Privacy Notices (published on the Academy websites) explain how data is collected and used.

Obtaining clear consent and ensuring that the consent remains in place is important for the Trust.

For Students and Parents/Carers

On joining an academy within the Trust you will be asked to complete a form giving next of kin details, emergency contact and other essential information. You will also be asked to give consent for the use of that information for other in Trust purposes, as set out on the data collection/consent form.

The contact and consent form will be reviewed on an annual basis. It is important to inform the Academy/Trust if details or your decision about consent changes.

Pupil consent procedure

Where processing relates to a child under 16 years old, the Trust will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

CCTV policy

Each academy has their own policy. The Trust may use CCTV and store images for a period of time in line with the CCTV Policy.

Data Protection Officer

We have a Data Protection Officer ("DPO") whose role is to:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

Our DPO is John Walker, who can be contacted at john@jawalker.co.uk

Complaints & the Information Commissioner Office (ICO)

Each Academy has a Complaints Policy which deals with complaints about Data Protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

There is also a right to complain is you have requested that data is erased, rectify or not processed and that request has not been adequately dealt with.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk
Helpline: 0303 123 1113
web: www.ico.org.uk

Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 12 months.