East Midlands Academy Trust

Data Protection and Data Retention Policy 2018/2019

'Every child deserves to be the best they can be'

Scope: EAST MIDLANDS Academy Trust & Academies within the Trust	
Version: 1	**Filename:** EAST MIDLANDS Academy Trust Data Protection and Data Retention Policy
Approval: October 2017	**Next Review: October 2019** *This policy will be reviewed every two years by the DSW Group and approved by the Board of Trustees.*
Owner: EAST MIDLANDS Academy Trust Board of Trustees	**Union Status:** Not applicable

Policy type:	
Statutory	Replaces Academy's current policy

Guidance:

The Guide to Data Protection (Information Commissioner's Office, 2015)

Cloud (Educational Apps) Software Services and the Data Protection Act - Departmental advice for local authorities, school leaders, school staff and governing bodies (DfE, 2014)

DATA PROTECTION POLICY

Introduction

EAST MIDLANDS Academy Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act (DPA) 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

This document sets out the obligations of The Trust with regard to data protection and the rights of people with whom it works in respect of their personal data under the Data Protection Act 1998 ("the Act").

This Policy sets out the procedures which are to be followed when dealing with personal data. These procedures must be followed by The Trust, its employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust.

The Trust views the correct and lawful handling of personal data as key to its success and dealings with third parties. The Trust shall ensure that it handles all personal data correctly and lawfully.

The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act established eight enforceable principles with which any party handling personal data must comply. All personal data:

1. Must be processed fairly and lawfully (and shall not be processed unless certain conditions are met)

2. Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes

3. Must be adequate, relevant and not excessive with respect to the purposes for which it is processed

4. Must be accurate and, where appropriate, kept up-to-date

5. Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed

6. Must be processed in accordance with the rights of data subjects under the Act

7. Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures and

8. Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Academy Response

The academy is committed to maintaining the above principles at all times. Therefore, in response, the academy will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (Appendix 1)
- Ensure our staff are aware of and understand our policies and procedures.

Rights of Data Subjects

Under the Act, data subjects have the following rights, to:

- be informed that their personal data is being processed
- access any of their personal data held by The Trust within 40 days of making a request
- prevent the processing of their personal data in limited circumstances and
- rectify, block, erase or destroy incorrect personal data

Personal Data

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Act also defines "sensitive personal data" as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Trust only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the data protection principles and with this Policy. Data related to employment, health and safety, safeguarding and education may be collected, held and processed by The Trust from time to time.

Processing Personal Data

Any and all personal data collected by The Trust (including that detailed later in this Policy) is collected in order to ensure that The Trust can facilitate efficient transactions with third parties including, but not limited to, students, parents and carers, partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. Personal data shall also be used by The Trust in meeting any and all relevant obligations imposed by law.

Personal data may be disclosed within The Trust. Personal data may be passed from one department to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any department or any individual within The Trust that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

The Trust shall ensure that all 8 Data Protection Principles (listed above) are applied consistently across the trust community:

- All personal data collected and processed for and on behalf of The Trust by any party is collected and processed fairly and lawfully
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)
- All personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed
- No personal data is held for any longer than necessary in light of the stated purpose(s)
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data
- All personal data is transferred using secure means, electronically or otherwise
- No personal data is transferred outside the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory; and
- All data subjects can exercise their rights set out above and more fully in the Act.

Cloud Computing

When considering data protection alongside potential take-up of cloud solutions, academies should be aware of the various challenges and responsibilities in respect of personal data that still remain (or indeed are created by this type of processing) . Whilst academy and childrens' data may be stored and controlled in the cloud by a supplier, responsibility for all areas of data protection compliance still rests with the particular academy.

Responsibilities

The Governors have overall responsibility for compliance with the DPA.

The Principal is responsible for ensuring compliance with the DPA and this policy within the day to day activities of the academy. The Principal is responsible for ensuring that appropriate training is provided for all staff.

When considering data protection alongside potential take-up of cloud solutions, schools should be aware of the various challenges and responsibilities in respect of personal data that still remain (or indeed are created by this type of processing). Whilst school and childrens' data may be stored and controlled in the cloud by a supplier, responsibility for all areas of data protection compliance still rests with the particular school.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in-line with the DPA. This compliance will be documented within the written contract between the school and the contractor; self-certification will not be acceptable.

Suppliers will be required to confirm their policy on advertisement-related data mining and advertisement-related profiling activities.

Complaints

Complaints will be dealt with in accordance with the academy's Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by EAST MIDLANDS Academy Trust.

Contacts

If you have any enquires in relation to this policy, please contact the Principal who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745.

Data Protection Procedures

The Trust shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust comply with the following when processing and / or transmitting personal data:

- All emails containing personal data must be encrypted;
- Personal data may be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances;
- Personal data should not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

- Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where Personal data is to be transferred in hardcopy form it should be passed

directly to the recipient. Using an intermediary is not permitted;

- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, including where accessed via the internet; and
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

Organisational Measures

The Trust shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer ("the Designated Officer") within The Trust shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust are made fully aware of both their individual responsibilities and The Trust's responsibilities under the Act and shall be made aware of the contents of this Policy.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
- The Performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust handling personal data shall be regularly evaluated and reviewed.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of The Trust handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, partners or other parties working on behalf of The Trust handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of The Trust arising out of this Policy and the Act.

- Where any contractor, agent, consultant, partner or other party working on behalf of The Trust handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless The Trust against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Access by Data Subjects

A data subject may make a subject access request ("SAR") at any time to see the information which The Trust holds about them.

Upon receipt of a SAR, The Trust shall have a maximum period of 40 days within which to respond. The following information will be provided to the data subject:

- Whether or not The Trust holds any personal data on the data subject
- A description of any personal data held on the data subject
- Details of what that personal data is used for
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

Notification to the Information Commissioner's Office

As a data controller, The Trust is required to notify the Information Commissioner's Office that it is processing personal data. The Trust is registered in the register of data controllers. Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

The Designated Officer shall be responsible for notifying and updating the Information Commissioner's Office.

Implementation of Policy

This Policy shall be deemed effective as of the date it is ratified by the Board. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

The Designated Officer has overall responsibility for the maintenance and operation of this policy. That person maintains a record of SARs and the outcomes and will report as necessary to board.

DATA RETENTION POLICY

The Information and Records Management Society (IRMS) is a professional association for those who work in records or information management. It has produced an information management toolkit for academies.

The toolkit shows the retention periods for different types of school records, and the actions to take at the end of a record's administrative life.

For some records, there are statutory retention periods. For others, retention guidelines follow best practice.

Managing records using these retention guidelines will be deemed as "normal processing" under the Data Protection Act 1998 and the Freedom of Information Act 2000.

If record series are to be kept for longer or shorter periods of time than laid out in this document the reasons for this need to be documented.

The IRMS toolkit has been created to assist academies to manage their information in line with current legislative frameworks.

The base toolkit is designed to assist academies in their compliance with the Freedom of Information Act 2000. Although the toolkit is aimed at maintained schools, academies also fall under the Freedom of Information Act and academies are data controllers in their own right. Although the toolkit has been designed as guidance and should "not be quoted to users as being a 'standard'", EAST MIDLANDS Academy Trust has adopted it as its standard.

http://www.irms.org.uk/images/resources/2016_IRMS_Toolkit%20for%20Schools_v5_Master.pdf

Retaining records: ICO

The Information Commissioner's Office (ICO) states that the Data Protection Act 1998 does not specify how long records should be kept for. It simply requires all schools, including academies, not to keep records for longer than necessary.

It recommends that academies can follow the IRMS toolkit for guidance when deciding how long to retain specific documents.

In line with ICO advice, this policy sets out for how long EAST MIDLANDS Academy Trust academies should keep different types of records and the reasons why it should keep them.

Retaining pupil records from primary academies

Secondary academies can receive many different files from primary academies and that two types of record – the 'pupil record' and the common transfer file – need to be retained until the pupil turns 25.

The pupil record is transferred from a pupil's primary to secondary school. Then that secondary school, or the school where the pupil goes on to complete his/her sixth form studies, is responsible for keeping that record until the pupil reaches the age of 25. Academies must retain the record for this length of time in order to comply with the Limitation Act 1980.

The files that should be part of the pupil record include, for example:

- Admission/application forms
- Privacy notices (if these are issued annually only the most recent need be on the file)
- Parental permission for photographs to be taken (or not)
- Annual written reports to parents
- Record sheets for the National Curriculum and the agreed religious education (RE) syllabus
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any information about a special educational needs (SEN) statement and support offered in relation to the statement
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

Schedule of Data Retention

GCSE student work stored on the network	1 year
A level student work stored on the network	1 year
Teacher work stored on the network	1 year
Support staff work stored on the network	1 year
KS3 student emails	1 year
KS4 student emails	1 year
Action plans	3 years
Principal reports	3 years
Attendance registers	3 years
Teacher emails	3 years
Support staff emails	3 years
Safeguarding lead work stored on the network	3 years
Principal's work stored on the network	3 years
Principal's emails	3 years

SLT work stored on the network	3 years
SLT emails	3 years
Business Manager work stored on the network	3 years
Business Manager emails	3 years
Finance Officer work stored on the network	3 years
Finance Officer email	3 years
Personnel and Finance Assistant work stored on the network	3 years
Personnel and Finance Assistant emails	3 years
Principal's PA work stored on the network	3 years
Principal's PA emails	3 years
SLT minutes	5 years
Internal examination results	5 years
Governance reports	6 years
Complaints files	6 years
Log books	6 years
CPD plans	6 years
Academy development plans	6 years
Admission registers	6 years
Public examination results	6 years
Annual reports (as required by DfE/EFA)	10 years
Governance agenda	Date of meeting

Policy document	Expiry of policy
Governance Minutes	Permanent
Instrument of governance	Permanent
Trusts and endowments	Permanent
Safeguarding lead emails	Until pupil reaches the age of 25
SEND Statements	Until pupil reaches the age of 30

Common transfer file

Secondary academies (or the school where the pupil completes sixth form studies) is responsible for keeping the common transfer file until the pupil reaches the age of 25.

Other types of files

The lengths of time for which academies should retain pupil records are shown on pages 49-51 of the IRMS toolkit.

EAST MIDLANDS Academy Trust advises keeping other files, which are not referred to in the IRMS toolkit, for "as long as necessary" and to take a common -sense approach before disposing of them. The above Schedule of Data Retention outlines the Trust approach.

Other types of files could also include non-statutory teacher assessment information, minor behavioural notes or information about the pupil's family.

Where possible, any information received from primary academies should be uploaded onto the academy's information management system during the autumn term.

Retaining information on staff no longer at the academy

The IRMS toolkit recommends that academies retain staff personal files for six years following the end of a staff member's employment, before 'secure disposal'. While most ordinary personnel files need to be kept for only six years from the termination of employment this should be considered to be the minimum retention period before reviewing (rather than disposing of) the file.

Some files may need to be kept for longer, for example if a staff member was involved in any child protection issues.

If pensionable information is kept on the personnel file, this will need to be retained until six years after the last pension payment has been made.

Different parts of the personal files of staff who have left the academy may have different retention periods. It is recommended that academies gradually remove parts of the file in accordance with their retention periods. Eventually, the file will just contain the employee's start date, end date, tax and pension information and whether or not he/she was dismissed.

Safe storage of staff and pupil records

Academies should consider the seventh principle of the Data Protection Act, which states:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

The ICO has published an overview of the requirements of the seventh principle of the Data Protection Act. In a section headed 'What kind of security measures might be appropriate?', it examines:

- What measures you may need to take at an organisational level
- How to ensure that staff are aware of their data protection responsibilities
- The security of premises and paper-based records
- Computer security

http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7#appropriate-measures

The ICO advises that hard copies of records should be safely secured in a lockable filing cabinet, and that electronic records should be password-encrypted.

Disposal of physical documents

While there is no official guidance on who can dispose of documents, it is the responsibility of each academy to dispose of its data in a secure manner, although there is no requirement for a particular member of staff to do so. Academies must ensure that this is done responsibly and securely.

Guidance on disposing of records

Pages 26-27 of the IRMS toolkit, linked to above, cover the safe disposal of records. It says that where an external provider is used, all records should be shredded on-site in the presence of an employee. Staff working for the external provider "should have been trained in the handling of confidential documents".

Where records are destroyed internally, a senior manager should authorise the destruction.

It also covers:

- The disposal of records that have reached the end of their minimum retention period
- The transfer of records to archives
- The transfer of information to other media
- The recording of all archiving, destruction and digitisation of records

Replacing hard-copy records with electronic records

Although there is no legislation on whether electronic records should replace hard-copy records, EAST MIDLANDS Academy Trust academies should ensure that where possible records are stored electronically on secure, encrypted media such as the academy network or a DfE-approved Cloud solution such as Microsoft Office 365.

Academies should convert paper records to digital media if the information needs to be kept for a long time. Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media.

It is essential to have procedures in place so that conversion is done in a standard way. This means that academies can prove that the electronic version is a genuine original and could not have been tampered with in any way.

Disposal of hard copies

Once information has been recorded electronically, it is the academy's choice whether to dispose of hard copies or not. If someone were to query an electronic record, an academy may be in a better position to confirm the accuracy of the electronic record if it were able to back it up with the original hard copy.

Academy closure

If the academy has been closed and the site is being sold or reallocated to another use, EAST MIDLANDS Academy Trust will take responsibility for the records from the date the academy closes.

If two academies have merged and function as one academy, it will be necessary for the new academy to retain any records originating from the two academies for the appropriate time.

If a school is converting to an academy, it should be treated as if the school has closed even though the academy may be reopening on the same site in the same buildings. The academy would be expected to take responsibility for the records relating to the pupils who have transferred to the academy and any records relating to the maintenance of buildings. The LA would take responsibility for all other records.

APPENDIX 1 – PROCEDURES FOR RESPONDING TO SUBJECT ACCESS REQUESTS MADE UNDER THE DATA PROTECTION ACT 1998

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request (SAR)

1. Requests for information must be made in writing; which includes email, and be addressed to the Principal. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- credit card or mortgage statement

(This list is not exhaustive)

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Principal should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The academy may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.

- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
  - If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Principal.

5. The response time for subject access requests, once officially received, is 40 days **(not working or academy days but calendar days, irrespective of academy holiday periods)**. However, the 40 days will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information, then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the academy with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the academy's complaint procedure.

Complaints which are not appropriate to be dealt with through the academy's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies/procedures, then please contact the Principal.

Further advice and information can be obtained from the Information Commissioner's Office www.ico.gov.uk