The

MAST

Academy Trust

Policy	Data Protection policy
Owner	The Mast Executive Administrator
Date approved	22nd June 2023
Approver	Audit Committee - Trust Board

Current version	V5.0

Next review due	Summer 2024

Objective of Policy

To provide guidance on the policy and process for data protection complying with the:

- Data Protection Act 2018
- Protection of Freedoms Act 2012
- GDPR 2018

Version Control	
Version Number	Summary of amends from previous version
2.0	Inclusion of Biometric data, front cover amends.
3.0	Annual review, updates to section 8.0, additional of appendices D & E
4.0	Annual Review
5.0	Annual Review

Sign off requirements	
Approvers	Position
Audit Committee	Trust Board
Reviewers	Position
Jason Field	CFO The MAST
Philip Marshall	Trustee

1.0 Introduction

The Mast Academy Trust Data protection and use of information policy sets out the principles for handling data responsibly and securely within our Trust and schools. This policy is also related to data concerning natural persons about whom we hold data (data subjects) and is designed to fulfil the requirements of the General Data Protection Regulation (GDPR) that came into force in May 2018.

Schools are obliged by law to fulfil the requirements of the GDPR and ensure that procedures are in place to satisfactorily assure that all areas of this policy are operating in practice.

In addition to this, the Trust is committed to ensuring that we have a safe data environment that respects the rights of all people that are affected by the scope of the GDPR and beyond. We will strive to continue making improvements in a changing data environment, and to challenge systems and individuals falling below the standards expected.

2.0 Key policy principles

- The Mast Academy Trust recognises that each of its schools is a public authority, as defined by the GDPR and must take accountability for this data and use of information policy in this context. As such we recognise that we are accountable for the data we control and have a responsibility to ensure those that process our data do so in line with the GDPR requirements.

- The Mast Academy Trust is serious about maintaining the highest standards of data management, ensuring that all people that are our data subjects are treated with respect and their rights are understood and held in high regard.

- The Mast Academy Trust will monitor its data environment and ensure that all data that we control or process is audited regularly and, if appropriate, assessment made as to the impact of data processing on our data subjects.

- Due regard will be given to the design of our systems, so as to ensure that the security of people's data is given high priority and that we will only hold data that is needed to lawfully and legitimately fulfil our organisation's operation. People within our organisation will only be given access to data that they need to carry out their roles and responsibilities at the school.

- We will uphold the rights of individuals to make legitimate requests for data, in a variety of categories as defined by the regulations and will respond to these requests reasonably and as laid out by the regulations.

- We will not hold data for longer than is reasonably needed and will dispose of time expired data in a suitable way given the level of sensitivity of the data.

- The Mast Academy Trust will ensure that the organisation has the necessary skills and support to respond to data requests, by having a suitably trained Data Protection Officer who will co-ordinate policy and procedures, respond to such requests and report to the Board of Trustees on progress against the requirements of the GDPR.

- Should any data breaches occur then these issues will be dealt with promptly and efficiently, as required by the GDPR, and The Mast Academy Trust will liaise with the Information Commissioner's Office (ICO), through the Data Protection Officer, and other agencies as directed in order to remedy these breaches and to learn lessons from any such breaches.

- The Mast Academy Trust will communicate with people that are classified as our data subjects (people about whom we hold data) and will inform them of what data we hold about them via privacy notices, what the lawful reason for holding this personal data is, and for how long we will hold the data. This is to ensure that our processes are transparent and that all people included in our data recording activities are treated fairly.

- The Mast Academy Trust will give training to all staff and other key stakeholders on data management, with regard to the scope of the GDPR and in order to ensure better data security, and to specific staff on the management of data where that is appropriate to their role.

- Should the standards we expect not be adhered to, accidentally or deliberately, then appropriate investigations will be conducted, recommendations made and remedial action taken, potentially including disciplinary action.

3.0 Our data

It will be the responsibility of The Mast Academy Trust to ensure that we have a clear understanding of any data that we hold with regards to our data subjects (as defined by the GDPR).

This data must be understood at a granular level and the reason for holding this data must be understood. Furthermore, a lawful reason for holding this data must be established and documented in order to ensure that our data subjects are protected from inappropriate use of their personal data and to minimise the risk of identity fraud.

An annual internal data audit throughout the Trust will be conducted to ensure that:

- our data records are up to date
- these records are complete and accurate
- any new data systems or processes have been included and their impact assessed
- any data due for destruction has been destroyed securely
- all requirements of the GDPR are being met

When carrying out the audit, the following should be considered:

A. all characteristics that are held with relation to the data subject
B. whether special category data is held
C. how long the data should be held for
D. What the lawful reason for holding the data is
E. what system the data is held on
F. who is responsible for managing that data system

Following the audit, any work required to ensure that all aspects of this policy are complied with should be carried out without undue delay, or an action plan be put in place to close any identified gaps.

4.0 Compliance with the GDPR and managing information responsibly

As the data controller for our information The Mast Academy Trust has a number of responsibilities with regard to ensuring that our data is compliant with the requirements of the GDPR. We will ensure that these responsibilities are upheld by complying with the GDPR and more specifically putting the following processes in place:

- Undertaking a data audit on an annual basis (as above) in order to ensure that we understand the data that we hold at all of the schools and have a record of our processing activities. Each school will be required to conduct a data audit annually.

- Reviewing the design of our data to ensure that we are minimising the risk of data breaches and that unnecessary data is not held in our systems

- Communicating with data subjects at least annually with reference to the data that we hold and why we hold it. This will be done through the issue of privacy notices, and in the case of our students these will be delivered via their parent/carers (for all children falling below the age of responsibility as defined by the GDPR and the ICO).

- Following a documented process to manage all data requests received from our data subjects and other parties that may request information from our organisation. This process will ensure that all the rights of the individual as laid out in the GDPR are respected and that timescales are adhered to.

- Appointing a trained Data Protection Officer who will be responsible for co-ordinating and implementing the policy of the Trust. They will ensure compliance across all the schools, report to the Board of Trustees on progress against the requirements of the policy and be the published contact point for requests for information. Refer to section 6 for more information.

- Contacting data processors in order to ensure that the requirements of the GDPR are in place. This will include, but is not limited to, information regarding the processing of data in international environments.

- Following a documented process to ensure that data breaches are recorded and appropriate decisions are made about communicating with the ICO and the data subjects of any such breach.

- Establishing data retention periods for each element of data and ensuring that destruction /deletion of data is undertaken as required.

- Explaining clearly the way in which data is used by data users in our organisation. Each user of data will be asked to record their understanding of their responsibilities. An acceptable use statement has been prepared for different information users so that it is clear to them how to use data in an acceptable way as a part of our school community.

- Providing guidance, best practice and requirements for ensuring that online safety is promoted and monitored in our schools. This is done in the best interests of the whole school community and is be reviewed regularly in order to ensure that the impact of developing technologies is taken into consideration.

5.0 Biometric Data

5.1 Key Points

Schools that use pupils' biometric data (see 5.2.1 below) must treat the data collected with appropriate care and must comply with the data protection principles as set out in the Data Protection Act 2018.

Where the data is to be used as part of an automated biometric recognition system (see 5.2.2 below), schools must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

Schools must ensure that each parent/carer of a child is notified of the school's intention to use the child's biometric data (see 5.2.1 below) as part of an automated biometric recognition system.

The written consent of at least one parent/carer must be obtained before the data is taken from the child and used (i.e. 'processed' – see 5.2.3 below). This applies to all pupils in schools under the age of 18. In no circumstances can a child's biometric data be processed without written consent.
Schools must not process the biometric data of a pupil (under 18 years of age) where:

- The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- No parent/carer has consented in writing to the processing; or
- A parent/carer has objected in writing to such processing, even if another parent/carer has given written consent.

Schools must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

5.2 What is biometric data?

5.2.1 Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data.

5.2.2 The Information Commissioner considers all biometric information to be sensitive personal data as defined by the GDPR 2018; this means that it must be obtained, used and stored in accordance with that Regulation.

5.2.3 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR 2018.

5.3 What is an automated biometric recognition system?

5.3.1 An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

5.3.2 Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 5.2.1 above.

5.4 What does processing data mean?

5.4.1 'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
b) Storing pupils' biometric information on a database system; or
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

6.0 Training and awareness

The training of staff and other users of data at the Mast Academy Trust and our schools will be given a high priority, to minimise the risk of inappropriate use of data, to minimise the risk of data breaches and promote the best practice in deliver the objectives of the trust and our schools whilst respecting the rights of our data subjects.

Training will be given on a regular basis and will include different messages for different staff and users of data. Staff or other users of data that handle specific or special category data will be given further training as necessary to ensure that they are fully aware of the impact that they might have if data is not handled appropriately.

We will also promote awareness amongst the whole community of data users and data subjects alike to ensure that there is an awareness of the need for balancing the needs of the school in controlling and processing personal data with the rights of individuals in protecting their own data.

7.0 Review

Our data environment is extremely dynamic meaning that review of our approach to information systems must remain under review and keep up to date with recent developments. This will mean that this policy will be updated at least annually and the schedules that inform the procedures that are in place for specific elements of our policy will be updated to reflect best practice and changing regulations.

8.0 Additional Information

- Acceptable use of ICT documents for data users – refer to the ICT and internet acceptable usage policy and information security guidance on the Mast Trust website
- Data audit template and record of processing activity – Held by the Data Protection Officer dataprotection@themast.co.uk – to be completed annually by each school.
- Data impact Assessment – Held by the Data Protection Officer dataprotection@themast.co.uk – to be completed on purchase of new information systems, by each school.
- Privacy notices – refer to the Privacy notices on the Mast Trust website
- Information request procedure – Refer to the Freedom of information policy on the Mast Trust website
- Data Breach Procedure – Held in each school office, contact school
- Data retention periods – Refer to Appendix D
- Detailed DPO job description – Refer to Appendix C
- Online safety guidance – Refer to the ICT and internet acceptable usage policy and information security guidance on the Mast Trust website.
- Data user and stakeholder responsibilities – Refer to Appendix E

APPENDIX A

NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION

Dear Parent/carer/Carer,

The school wishes to use information about your child as part of an automated (i.e. electronically-operated) recognition system. This is for the purposes of [specify what purpose is – e.g. catering, library access]. The information from your child that we wish to use is referred to as 'biometric information' (see next paragraph). Under the Protection of Freedoms Act 2012 (sections 26 to 28), we are required to notify each parent/carer of a child and obtain the written consent of at least one parent/carer before being able to use a child's biometric information for an automated system.

Biometric information and how it will be used: Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their [fingerprint/iris/palm]. The school would like to take and use information from your child's thumbprint and use this information for the purpose of providing your child with school lunches. The information will be used as part of an automated biometric recognition system. This system will take measurements of your child's thumbprint and convert these measurements into a template to be stored on the system. An image of your child's thumbprint is not stored. The template (i.e. measurements taking from your child's thumbprint is what will be used to permit your child to access services.

You should note that the law places specific requirements on schools when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system. For example: (a) the school cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent/carer(s) (i.e. as stated above); (b) the school must ensure that the information is stored securely; (c) the school must tell you what it intends to do with the information; (d) unless the law allows it, the school cannot disclose personal information to another person/body – you should note that the only person/body that the school wishes to share the information with is the Trust's chosen cashless till system supplier with whom the information is to be shared. This is necessary in order to allow pupils to pay for their school meal.

In order to be able to use your child's biometric information, the written consent of at least one parent/carer is required. However, consent given by one parent/carer will be overridden if the other parent/carer objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school cannot collect or use their biometric information for inclusion on the automated recognition system. You can also object to the proposed processing of your child's biometric information at a later stage or withdraw any consent you have previously given. This means that, if you give consent but later change your mind, you can withdraw this consent. Please note that any consent, withdrawal of consent or objection from a parent/carer must be in writing. Even if you have consented, your child can object or refuse at any time to their biometric information being taken/used. Their objection does not need to be in writing. We would appreciate it if you could discuss this with your child and explain to them that they can object to this if they wish.

The school is also happy to answer any questions you or your child may have. If you do not wish your child's biometric information to be processed by the school, or your child objects to such processing, the law says that we must provide reasonable alternative arrangements for children who are not going to use the automated system to access school meals. If you give consent to the processing of your child's biometric information, please sign, date and return the enclosed consent form to the school. Please note that when your child leaves the school, or if for some other reason he/she ceases to use the biometric system, their biometric data will be securely deleted.

Please complete this form if you consent to the school taking and using information from your child's thumbprint by <school> as part of an automated biometric recognition system. This biometric information will be used by <school>for the purpose of paying for school lunches. In signing this form, you are authorising the school to use your child's biometric information for this purpose until he/she either leaves the school or ceases to use the system. If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school at the following address:

School contact details

Once your child ceases to use the biometric recognition system, his/her biometric information will be securely deleted by the school. Please send the completed form to the School Office.

CONSENT FORM FOR THE USE OF BIOMETRIC INFORMATION IN SCHOOL

Having read guidance provided to me by <school>, I give consent to information from the thumbprint of my child:

Child's Name……..

being taken and used by <school> for use as part of an automated biometric recognition system for school meals for which this data will be used, I understand that I can withdraw this consent at any time in writing.

Name of Parent/carer: …….

Signature: …….

Date: ……

APPENDIX B

What information should schools provide to parent/carers/pupils to help them decide whether to object or for parent/carers to give their consent?

Any objection or consent by a parent/carer must be an informed decision – as should any objection on the part of a child. Schools should take steps to ensure parent/carers receive full information about the processing of their child's biometric data including a description of the kind of system they plan to use, the nature of the data they process, the purpose of the processing and how the data will be obtained and used. Children should be provided with information in a manner that is appropriate to their age and understanding.

What if one parent/carer disagrees with the other?

Schools are required to notify each parent/carer of a child whose biometric information they wish to collect/use. If one parent/carer objects in writing, then the school will not be permitted to take or use that child's biometric data.

How will the child's right to object work in practice – must they do so in writing?

A child is not required to object in writing. An older child may be more able to say that they object to the processing of their biometric data. A younger child may show reluctance to take part in the physical process of giving the data in other ways. In either case the school will not be permitted to collect or process the data.

Are schools required to ask/tell parent/carers before introducing an automated biometric recognition system?

Schools are not required by law to consult parent/carers before installing an automated biometric recognition system. However, they are required to notify parent/carers and secure consent from at least one parent/carer before biometric data is obtained or used for the purposes of such a system. It is up to schools to consider whether it is appropriate to consult parent/carers and pupils in advance of introducing such a system.

Do schools need to renew consent every year?

No. The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time if another parent/carer or the child objects to the processing (subject to the parent/carer's objection being in writing). When the pupil leaves the school, their biometric data will be securely removed from the school's biometric recognition system.

Do schools need to notify and obtain consent when the school introduces an additional, different type of automated biometric recognition system?

Yes, consent must be informed consent. If, for example, a school has obtained consent for a fingerprint/fingertip system for catering services and then later introduces a system for accessing library services using iris or retina scanning, then schools will have to meet the notification and consent requirements for the new system.

Can consent be withdrawn by a parent/carer?

Parent/carers will be able to withdraw their consent, in writing, at any time. In addition, either parent/carer will be able to object to the processing at any time but they must do so in writing.

When and how can a child object?

A child can object to the processing of their biometric data or refuse to take part at any stage – i.e. before the processing takes place or at any point after his or her biometric data has been obtained and is being used as part of a biometric recognition system. If a pupil objects, the school must not start to process his or her biometric data or, if they are already doing this, must stop. The child does not have to object in writing.

Will consent given on entry to the school be valid until the child leaves that school?

Yes. Consent will be valid until the child leaves the school – subject to any subsequent objection to the processing of the biometric data by the child or a written objection from a parent/carer. If any such objection is made, the biometric data should not be processed and the school must, in accordance with the Data Protection Act, remove it from the school's system by secure deletion.

Can the school notify parent/carers and accept consent via email?

Yes – as long as the school is satisfied that the email contact details are accurate and the consent received is genuine.

Will parent/carers be asked for retrospective consent?

No. Any processing that has taken place prior to the provisions in the Protection of Freedoms Act coming into force will not be affected.

Does the legislation cover other technologies such a palm and iris scanning?

Yes. The legislation covers all systems that record or use physical or behavioural characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parent/carer notification and consent required under the Protection of Freedoms Act 2012 for the use of photographs and CCTV in schools?

No – not unless the use of photographs and CCTV is for the purposes of an automated biometric recognition system. However, schools must continue to comply with the requirements in the Data Protection Act 1998 (DPA) when using CCTV for general security purposes or when using photographs of pupils as part of a manual ID system or an automated system that uses barcodes to provide services to pupils. Depending on the activity concerned, consent may be required under the DPA before personal data is processed. The Government believes that the DPA requirements are sufficient to regulate the use of CCTV and photographs for purposes other than automated biometric recognition systems. Photo ID card systems where a pupil's photo is scanned automatically to provide him or her with services would come within the obligations on schools under sections 26 to 28 of the

Protection of Freedoms Act 2012 as such systems fall within the definition in that Act of automated biometric recognition systems.

Is parent/carer notification or consent required if a pupil uses or accesses standard commercial sites or software which use face recognition technology?

The provisions in the Protection of Freedoms Act 2012 only cover processing by or on behalf of a school. If a school wishes to use such software for school work or any school business, then the requirement to notify parent/carers and to obtain written consent will apply. However, if a pupil is using this software for their own personal purposes then the provisions do not apply, even if the software is accessed using school equipment.

Institute guide to biometrics: http://shop.bsigroup.com/en/Browse-by-Subject/Biometrics/?t=r

APPENDIX C

Role description: Data Protection Officer (DPO)

Purpose

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes and advise the Trust and our schools on best practice.

Key responsibilities

To:

- Advise the Trust, our schools and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Develop an in-depth understanding of the Trust's and each school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the Trust's and each school's compliance with data protection law, by:
    - Collecting information to identify data processing activities
    - Analysing and checking the compliance of data processing activities
    - Informing, advising and issuing recommendations to the school
    - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the Trust's and each school's policies are followed, through:
    - Assigning responsibilities to individuals
    - Awareness-raising activities
    - Co-ordinating staff training
    - Conducting internal data protection audits
- Advise on and assist the Trust and each school's with carrying out data protection impact assessments, if necessary
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information
    - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example, staff, pupils and parent/careers), including:
    - Responding to subject access requests
    - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focusing mostly on these

    - Advising the Trust or the school if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve
- Report to the *[governing board/board of trustees]* on the *[Trust's or school's]* data protection compliance and associated risks
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role
- Undertake any additional tasks necessary to keep the Trust and each school compliant with data protection law and be successful in the role

[The above are the requirements for the DPO role as set out in the GDPR. You may wish to add in your own responsibilities depending on your context and needs. We have provided some examples below.]

- Maintain a record of the Trust and each school's data processing activities
- Work with external stakeholders, such as suppliers or members of the community, on data protection issues
- Take responsibility for fostering a culture of data protection throughout the Trust and each school
- Work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security

Notes for internal candidates

Internal staff members may take on this role, but before expressing an interest should be aware that the DPO must:

- Be a senior member of staff, reporting to the *[board of governors/board of trustees]*
- Have a role which is compatible with the DPO role, in terms of time and workload
- Not have any conflicts of interest between their current role and the DPO role

Person specification

Criteria	Desirable qualities
Qualifications	• Background in information security, data protection or IT desired • Educated to degree level, or equivalent professional experience • Relevant data protection qualification desired *[You will need to use your own judgement to determine the qualifications your DPO needs to have, depending on your data protection needs]*
Experience	• Professional experience of data protection law • Experience of managing data protection compliance, particularly responding to subject access requests *[You will need to use your own judgement to determine the experience your DPO needs to have, depending on your data protection needs]*
Skills and knowledge	• Knowledge of data protection law (the GDPR and Data Protection Act 1998) • Knowledge of information security and data processing principles and good practice • An understanding, and prior use of the following systems: ○ *[Insert any data systems your school uses e.g. MIS, computer operating systems, data security systems]* • Excellent communication skills • Excellent teamwork and interpersonal skills, with proven ability to maintain relationships across a school or other organisation • Ability to explain complex data protection and information security information to a non-specialist audience
Personal qualities	• Detail-oriented • Ability to work under pressure • Ability to prioritise tasks effectively • Ability to work independently and autonomously with minimal supervision • Commitment to maintaining confidentiality at all times

Appendix D: Data retention - Schedule and Guidance

The Trust and its schools take care to store data for a period of time that reflects their needs but equally protects the rights of individuals. However, there are still legal considerations in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and
- the General Data Protection Regulation (from May 25th 2018).

These inform not only retention periods, but also what to keep and who should be able to access it.

On 25th May 2018, the General Data Protection Regulation came into effect across the UK.

Introduction

Reasons to keep certain records, such as child protection records, for many years after pupils or staff leave the trust/school need to be weighed against personal rights and be supported by a lawful reason. Longer retention of data, particularly special category data mean that our schools will put in place more secure storage systems and protocols in place.

The Trust and its schools take steps to ensure its retention policies are communicating the reasons for the policy in privacy notices and staff or parent/carer contracts and are ensuring any records necessary to keep long term are kept very secure, accessible only by trained staff who require this information to perform their official function.

Personal data is kept for a period of time as defined below, with statute for the retention of records being a key factor in many decisions in the length of retaining data. Annual data review schedules are undertaken to ensure that records no longer required are disposed of appropriately.

1. Archiving and the disposal or erasure of Records

All staff receive basic training in data management – issues such as security, recognising and handling personal data, safeguarding etc. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, the following:

- That records – whether electronic or hard copy – are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required;
- That important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks, personal servers / data storage or mobiles and handheld electronic tablets) unless absolutely necessary, in which case it should be subject to a risk assessment and in line with an up-to-date IT acceptable use policy;
- That questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action;
- That arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – are supported by robust contractual arrangements providing for security and access;

- That information storage systems will, over time, be enhanced to allow erasure of records to be more efficient and granular over time. This will form part of review processes on a periodic basis;
- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and
- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.
- This is particularly important in respect of the Trust's and each school's specific legal obligations under the GDPR. However, they amount to common sense rules even where personal data is not directly involved. This is also supported by our acceptable use of ICT policy.

2. Retention periods

Consideration is given as to how long each category of record should be kept. In particular, statutory guidance will be taken into account with regard to particular types of record (e.g. Safeguarding information, financial invoices) to ensure that the Trust and each of our schools are able to have a strong organisational memory that allows us to recall vital information.

The Schedule below is guided by these principles and where there is no statutory guidance is in place the data is be held to support our organisational memory with respect to key decisions, balancing this with the rights of individuals.

In some cases the prompt for disposal may be the end of a calendar year or financial year, meaning that disposal dates will not be exact and the annual cycle of activity will need to be taken into consideration.

Should the Trust or a school have particular reasons for retaining data beyond the periods laid out in the schedule (e.g. pending court action / ongoing investigation) then periods may be extended, supported by evidence to validate that decision.

3. Recording information

All staff must be clear, when creating documents and records of any sort (including email), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a subject access request under the GDPR. All records must be, amongst other things, be accurate, clear, professional and objective.

4. Secure disposal of documents

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal will not be considered secure.

Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed.

Where third party disposal experts are used they should ideally be supervised but, in any event, be under adequate contractual obligations to the Trust or a school to process and dispose of the information securely.

5. Rules applicable to child protection (CP) files

Often CP files will comprise personal, special category or sensitive personal data (e.g. physical or mental health, sexual life or criminal allegations). Recent 'historic' cases in the field of child protection make a cautious approach to record retention advisable and, from a GDPR perspective, make it easier for a school to justify retention for long periods – even the lifetime of former staff and pupils.

- Child protection concerns, disclosures, referrals, etc relating to individual children must be recorded, stored and maintained as described in 'Keeping children safe in education' (DfE 2016) – no child protection / safeguarding information should be recorded in a child's educational records;
- The CP files must be stored in a locked cabinet or – if electronic – in a secure format, with controlled access only to the Designated staff and Head Teacher. If the records need to be viewed by another person (e.g. a member of pastoral staff, inspector, police) a record should be made on the chronology of the date, the identity of the person and the purpose;
- If using an electronic CP recording system, the provider must give assurances that the appropriate security certificates are in place. Staff should not pass cause for concern notifications to the DSL via email but via the designated system;
- Each pupil should have their own file; no "family" files should be kept. The front of the file should include a sheet detailing contact details of those with parent/carer rights, other significant adults in the household, any allocated social worker or other agencies involved, etc. Each file should also include a chronology of key events;
- If a child leaves school to move to another school or an FE college, the CP file should be transferred securely to the new Designated Safeguarding Lead as soon as possible. Ideally this will be by face to face handover (with electronic files being via a secure transmission protocol); if it is necessary to post the file this should be by secure mail and the new DSL should be notified to expect it. A copy should be retained by the school however, and archived in the manner below;
- When a child leaves the school for any reason, the CP file should be archived in line with the following retention schedule:
    - If the file contains low level concerns that have never led to a referral to partner agencies – retain until the pupil's 25th birthday (or the end of that academic year);
    - If a referral was ever made to children's social care or the child is or has been looked after – review retention of the record to reflect the need for that record based on potential risk to the child;
- In the event that a parent/carer or pupil requests sight of the CP file the school should seek advice from the Headteacher or Data Protection Officer without delay. Parent/carers do not always have an automatic right to access their child's personal information under a Subject Access Request: if the child is old enough to make the decision (determined to be the age of 13), then it is the child's decision whether his or her parent/carers should exercise the right under data protection law to access his or her personal data.
- It is within the protocols of handling this data that information pertinent to a child should be handed over (with a secure audit trail) to the child's next educational establishment thus avoiding duplication of records and further risk of data breach.
- Please note that IICSA (Independent Inquiry into Child Sexual Abuse) has issued very strong guidelines on not destroying or deleting files which may be of interest to the Inquiry, whether or not a school has received a letter from IICSA. How a school handles records and concerns raised may be within the scope of the Enquiry, even if there was no major incident. It is expected that the final report produced by IICSA will contain recommendations about recording, retention and storage that may become law but until then a cautious approach to retention is advisable.

TABLE OF RETENTION PERIODS

Type of Record/Document	Suggested [1] Retention Period
SCHOOL-SPECIFIC RECORDS	
Registration documents of School	Permanent (or until closure of the school)
Attendance Register	6 years from last date of entry, then archive.
Minutes of Governors' meetings	10 years from date of meeting
Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	*NB – this will generally be personal data*
Admissions: • *Admission file* • *Admission appeals*	1 year after pupil leaving school
Attainment • *Attainment data, test results*	5 years after pupil leaving school
Attendance data	5 years after pupil leaving school
Record of absence	1 year after pupil leaving school
Record of exclusion	1 year after pupil leaving school (transferred to new setting with transfer file)
Behaviour information • *General Behaviour incidents*	1 year after pupil leaving school (transferred to new setting with transfer file)
Trips and activities • *Trip information, consent and visitors record*	Immediately after trip or visit
Financial records from trip	6 years in line with other financial records
Record of major incidents	Until pupil reaches age of 25 (subject to individual case risk assessment)
Medical information • *Permission to administer medicine*	1 month after end of medication being administered
Medical conditions and ongoing mgt	1 year after pupil leaving school
Serious medical incidents	Until pupil reaches age of 25 (subject to individual case risk assessment)
Safeguarding records (to be risk assessed individually) *A. Safeguarding records with no referrals to other agencies* *B. Safeguarding records referred to other agencies*	A. 5 years from date of birth B. Minimum 25 years from date of birth then undertake risk review *C.* Minimum 25 years from date of birth then undertake risk review

C. *Safeguarding records of Children that have been looked after*	*Note that these records should be passed on (with a verification of handover) to the next environment in which the child is being educated – no personal data records should be retained in the school after the child has left*
SEN records • *Records of Special Educational needs*	• 25 years from date of birth *Note that these records should be passed on (with a verification of handover) to the next environment in which the child is being educated – no personal data records should be retained in the school after the child has left*
Other pupil information *A. Photographic identifier in Management information System (for identification)* *B. Other photographic information (e.g. for publicity / social media)* *C. Name and Address* *D. Pupil characteristic information* *E. Parent/carer contact and status information* F. *Biometric information (catering)*	A. 1 year after pupil leaving school B. In line with specified consent C. 1 year after pupil leaving school D. 1 year after pupil leaving school E. 1 year after pupil leaving school F. In line with consent (whilst data is actively in use)
SAFEGUARDING	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
Child Protection files	Low level concerns, no multi-agency act - 25 years from date of birth; for other instances see above
FINANCIAL RECORDS	
Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state e.g. invoices / VAT records etc.)	6 years from the end of the financial year in which the transaction took place
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
Insurance records	Minimum – 7 years
CONTRACTS AND AGREEMENTS	

Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
EMPLOYEE / PERSONNEL RECORDS	*NB this will almost certainly be personal data*
Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken. For former staff this will be in their employment file, for current staff this will be in the SCR.
Contracts of employment	7 years from effective date of end of contract
Employee appraisals or reviews	7 years from effective date of end of contract
Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims. Allegations of abuse will be kept for 10 years or to retirement age whichever is longer
Payroll, salary, maternity pay records	6 years
Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
Immigration records	4 years
Health records relating to employee	7 years from effective date of end of contract
ENVIRONMENTAL & HEALTH RECORDS	
Accidents to children 25 years from birth (unless safeguarding incident)	25 years from birth (additional review for safeguarding incidents)
Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case
Staff use of hazardous substances	7 years from end of date of use
Risk assessments	7 years from completion of relevant project, event or activity.
Asbestos register and plan	Permanent

Note: all records are subject to review prior to destruction and any records being retained will be accompanied by a documentary justification for additional retention.

APPENDIX E - Key responsibilities

Introduction

We all have responsibilities for protecting personal data and using information responsibly. To ensure that this happens on a consistent basis throughout our organisation this will be made clear to all that are part of our data ecosystem, and specific responsibilities will be given to ensure there is clarity around accountability and responsibility for particular areas of implementing the policy.

The responsibilities of the various parties affected by this policy are as follows:

A. Board of Trustees

The Board of Trustees of The Mast Academy Trust is ultimately responsible for ensuring that the Data protection and use of information policy in place complies with the General Data Protection Regulation and satisfies other guidance relating to the use of information in schools.

They will monitor the policy and ensure recommendations and reports submitted to them by the ICO or Data Protection Officer are given due consideration and action taken as necessary.

The Board of Trustees will receive information regarding any data breaches and information requests relating to the Trust or our schools during the course of the year and ensure that action is being taken to maintain high standards of data management.

The Board of Trustees will review the data protection and use of information policy and its schedules on a periodic basis to ensure that the policy remains coherent and up to date.

The Board of Trustees will also be asked to ensure the oversight of the implementation of any actions as agreed at meetings from time to time.

The Board of Trustees will be responsible for appointing the Data Protection Officer

B. Local Governing Body

The Local Governing Body is responsible for ensuring that the principles of data protection and use of information are applied at the school.

This includes monitoring the policy on a periodic basis to ensure that standards are in place relating to the protection of personal data and use of information in the school.

The Local Governing Body has the authority to scrutinise the arrangements for data protection at the school and will receive on an annual basis a report from the Data Protection Officer with regard to the suitability of internal controls at the school.

C. Headteachers

Headteachers are responsible for reporting to the Trust with respect to the operation of the data protection and use of information at school policy at school level and updating the LGB on any actions as requested.

Headteachers are also responsible (and may delegate this responsibility to suitably qualified staff) for ensuring that only necessary access to data is given to all members of the school's community (e.g. pupils / staff / governors / visitors / contractors).

Headteachers are responsible for ensuring all users of data in the school (including visitors) are given appropriate training and/or information to ensure compliance with regulations and the highest standards of information security.

Headteachers are responsible for liaising with the Data Protection Officer in the case of any personal data breach and will report this to the Trust if it is decided serious enough to be reported to the Information Commissioners Office.

Headteachers are responsible for organising investigations into inappropriate use of information and ensuring actions are taken to minimise the risk of re-occurrence.

Headteachers are responsible for recording data breaches and requests for information on the logs provided by the Trust.

D. Data Protection Officer

The Data Protection Officer has specific responsibilities laid out in the General Data Protection Regulation. The principles of these are laid out below:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, pupils / parent/carers, customers etc).

In carrying out these responsibilities, the Data Protection Officer will report to the Board of Trustees and submit reports and recommendations regarding the operation of the policy. The Board of Trustees will ensure that the Data Protection Officer is protected from any disciplinary action with regards to carrying out their duty with regards to the GDPR.

The Data Protection Officer will be appointed and will work under the direction of the Board of Trustees, having access to inform this decision making body directly.

The Data Protection Officer will provide support and documentation to schools and headteachers in order to ensure that the administrative processes associated with GDPR and data management are as clear as possible.

E. Third- party data processors

Where external companies are used to process personal data on behalf of the school, accountability for the security and appropriate use of that data remains with the school and ultimately the LGB.

Where a third-party data processor is used:

- a data processor must be chosen providing sufficient guarantees and evidence about its ability to protect the personal data of the data controller's data subject.
- reasonable steps must be taken that such security measures are in place, including written or contractual evidence that data security measures are in place with regards to relevant data.
- Further assurances regarding data processed outside of the United Kingdom must be sought in order to ensure that appropriate security is in place for the processing of this data.

F. Pupils and other children accessing data

Pupils will be given clear guidance on the acceptable use of information within their school life. It is their responsibility to adhere to these guidelines and ensure that they follow the school's guidance in this area.

They are expected to adhere to all of this guidance and any breaches will be investigated and further action may be taken.

Further details of what their responsibilities with regard to this can be found in the Acceptable use of IT schedule.

G. Staff

Staff and other users may be given access to data and use this in the course of doing their work or employment. It is their responsibility to ensure that data that they have access to will be treated within the guidelines outlined. Each of these individuals will be given training on the use of data and protecting the rights of data subjects. Failure to comply may result in disciplinary action against the individual.

H. Other users of information

Other users of information in the school must be given guidance on what information they are able to access. This will be designed to absolutely minimise access to personal data and will be within a clearly defined lawful reason, supported by a data sharing agreement where appropriate. When being given access to this information the school will monitor that this information is the only information being accessed. It is the responsibility of these users to access only the information agreed and misuse of information will lead to corrective action up to and including legal action and remedies.