The

MAST

Academy Trust

Policy	Data Protection policy		
Owner	Melanie Humphreys – The Mast Executive Administrator		
Date approved	27th March 2020	**Adopted from**	March 2020
Approver	Martyn Jones	**Signature**	Martyn Jones

Current version	V2.0 March 2020

Next review due	Spring Term 2021

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.

Sign off requirements	
Approvers	Position
Chair of trustees ratification	Martyn Jones
Local LGB adoption approval	Chair of Governors per LGB
Reviewers	Position
Jason Field	CFO The MAST
Philip Oldfield	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 its schools. This policy is also related to data concerning natural persons about whom we hold data and is designed to fulfil the requirements of the General Data Protection Regulations (GDPR) that come 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. Constant improvements in a changing data environment will be strived for, and systems and individuals falling below the standards expected will be challenged.

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 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 skill 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 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 Commissioners Office, 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 who we hold data about) and will inform them of what data we hold about them via privacy notices and what the lawful reason for holding this personal data is, and for how long we will hold the data. This will 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 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 our school expects not be adhered to, accidentally or deliberately, then appropriate investigation 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 initial data audit will be conducted to establish what data is being held and whether or not the data held complies with the requirements of the GDPR. This audit will be a detailed exercise and will establish a number of factors including:

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
G. How long the data will be held for

Once the initial data audit is conducted further work will be done to ensure that all aspects of this policy are complied with, or that an action plan is in place to close gaps. A further audit will be conducted annually, with the aim of bringing the records of what data is held up to date, ensuring accuracy of those records and to ensure that new data systems have been included and their impact assessed and that data due for destruction has been destroyed securely.

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 will be delivered via their parents (for all children falling below the age of responsibility as defined by the GDPR and the ICO for the UK).

- Putting a process in place for managing all data requests received from our data subjects and others 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.

- The Mast Academy Trust will appoint a 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.

- The Mast Academy Trust will contact data processors in order to ensure that the requirements of the GDPR are being put in place. This will include, but is not limited to, information regarding the processing of data in international environments.

- A documented process will be put in place in order to ensure that data breaches are recorded and decisions made about communication with the Information Commissioners Office and the data subjects of any such breach.

- Data retention periods for each element of data identified in the data audit process will be established and as part of the annual audit appropriate destruction /deletion of this data will be undertaken.

- The way in which data is used by data users in our organisation will be explained clearly and each user of data will be asked to record their understanding of their responsibilities. An acceptable use statement will be 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.

- We will provide guidance, best practice and requirements for ensuring that online safety is promoted and monitored in ours school. This will be done in the best interests of the whole school community and will 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 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 1998.

Where the data is to be used as part of an automated biometric recognition system (see 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 of a child is notified of the school's intention to use the child's biometric data (see 2.1 below) as part of an automated biometric recognition system.

The written consent of at least one parent must be obtained before the data is taken from the child and used (i.e. 'processed' – see 2.3 below). This applies to all pupils in schools and colleges 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 has consented in writing to the processing; or
- A parent has objected in writing to such processing, even if another parent has given written consent.

Schools and colleges 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 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 and colleges 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 our school 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 school 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 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. This will be done annually as a minimum.

8.0 Additional Information:

Acceptable use of ICT documents for data users – individual schools to update

Data audit template and record of processing activity – individual schools to update

Data impact Assessment – **Held by ICT Manager for the Mast Academy Trust**

Privacy notices – individual schools to update

Information request procedure –**Freedom of Information Policy**

Data Breach Procedure – **Held by ICT Manager for the Mast Academy Trust**

Data retention periods – individual schools to update

Detailed DPO job description –**Appendix C**

Online safety guidance – individual schools to update

Data user and stakeholder responsibilities – **Held by ICT Manager for the Mast Academy Trust**

APPENDIX A

NOTIFICATION OF INTENTION TO PROCESS PUPILS' BIOMETRIC INFORMATION

Dear Parent/Carer,

The school/college 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 of a child and obtain the written consent of at least one parent 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 and colleges when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system. For example: (a) the school/college cannot use the information for any purpose other than those for which it was originally obtained and made known to the parent(s) (i.e. as stated above); (b) the school must ensure that the information is stored securely; (c) the school/college 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 Nationwide Cashless Tills System with which the information is to be shared. This is necessary in order to allow pupils to pay for their school meal.

Providing your consent/objecting as stated above, in order to be able to use your child's biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if your child objects to this, the school/college cannot collect or use his/her 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 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.

His/her 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/college. Please note that when your child leaves the school/college, or if for some other reason he/she ceases to use the biometric system, his/her 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 Scissett Middle School as part of an automated biometric recognition system. This biometric information will be used by Scissett Middle 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/college 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: …….

Signature: …… Date: ……

APPENDIX B

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

Any objection or consent by a parent must be an informed decision – as should any objection on the part of a child. Schools and colleges should take steps to ensure parents 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 disagrees with the other?

Schools are required to notify each parent of a child whose biometric information they wish to collect/use. If one parent 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 parents before introducing an automated biometric recognition system?

Schools are not required by law to consult parents before installing an automated biometric recognition system. However, they are required to notify parents and secure consent from at least one parent 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 parents 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 or the child objects to the processing (subject to the parent'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?

Parents will be able to withdraw their consent, in writing, at any time. In addition, either parent 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 a the middle 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. 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 parents 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 parents 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 behavioral characteristics for the purpose of identification. This includes systems which use palm, iris or face recognition, as well as fingerprints.

Is parental 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 and colleges 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 parental 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 parents 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 school on best practice.

Key responsibilities

To:

- Advise the school 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 school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the 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 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 school 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 parents), 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 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 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 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 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 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