SHARE
MULTI-ACADEMY TRUST

GENERAL DATA PROTECTION REGULATION POLICY

GDPR POLICY TO BE USED BY ALL SCHOOLS IN THE TRUST

Version	2.1
Name of Policy Writer	Debbie Howard
Review date	October 2022
Approved by Directors	3rd October 2019
ICO Reg Number	Z2844414

Record of Alterations

Version 1.0	Original
Version 2.0	Amendments
Version 2.1	Reviewed April 2021 with no amendments

CONTENTS

1. Overview

SHARE MAT aims to ensure that all its processes and procedures are in line with all relevant forms of data protection legislation. As part of the General Data Protection Regulation, the trust is required by law to outline its aims in response to the GDPR.

In addition to the 'GDPR Policy' the trust also has a full suite of policies accessible via the website, the school's website and internal shared drives.

2. Purpose

The purpose of this policy is to inform data subjects about the trust's processes and procedures which are carried out in accordance with GDPR. All personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, including paper and electronic format.

3. Legislation and guidance

It is a requirement for all Schools and Public Authorities to adhere to the GDPR and Data Protection legislation, set out in the Data Protection Law (1998) and the General Data Protection Regulation (2018).

This policy:

- is based on the guidelines set out by the Information Commissioners Office (ICO) and The General Data Protection Regulation (2018) and Data Protection (1998) legislations. It also follows the guidance of the Protection of Freedoms Act (2012) and the Freedom of Information Act (2000) to ensure the protection of biometric data.
- complies with the trust's funding agreements and articles of association.
- meets the requirements of the Protection of Freedoms Act 2012 when referring to use of biometric data.
- reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational records.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. Personal data is only associated with a living data subject. This may include the individual's: • Name (including initials) • Identification number • Location data • Financial data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and therefore needs further protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Actions done to personal data, such as; • Collecting • Recording • Organising • Structuring • Sharing • Storing • Adapting • Altering • Retrieving • Using • Disseminating • Erasing • Destroying Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed. A data subject is any natural, living person.

Data Controller	A person and/or organisation that determines the purposes and the means of processing personal data.
Data Processor	A person, organisation or other body (other than an employee of the data controller) who processes personal data on behalf of the data controller.
'DPO'	'DPO' is an abbreviation of the term, Data Protection Officer. A DPO should be appointed when any large-scale processing of data occurs, and/or, processing of data may be deemed a risk.
Personal Data Breach or Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
The ICO	The Information Commissioners Office - the authority who manages GDPR and Data Protection.
A DPIA (Data Protection Impact Assessment)	A DPIA is an activity undertaken in order to assess whether an organisation is carrying out process in line with relevant legislation.
SAR/DSAR	A 'SAR' or sometimes referred to as a 'DSAR', is an abbreviation of the world Subject Access Request. This is when a data subject formally lodges a request to view/ access stored data which is personal to them.

5. The data controller

The trust processes personal data relating to parents, students, staff, governors, visitors and others. Under GDPR, the trust (and all of the schools within the trust) is a data controller.

The trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. Roles and responsibilities

This policy applies to all staff employed by the trust and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 Governing Board

The governing board has overall responsibility for ensuring that the trust complies with all relevant data protection obligations.

6.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the trust's compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the governing board and, where relevant, report to the board to offer their advice and recommendations on school's data protection issues.

The DPO will manage risk across all of the schools within the trust, assessing all levels of risk and implementing better practise to mitigate these risks.

The DPO will manage all Data Breaches and near misses across all of the schools within the trust. With the support of the Admin Managers and all parties involved within a breach, the DPO will produce reports and action plans for all breaches that occur.

The DPO is also the first point of contact for individuals whose data the trust processes, and for the ICO.

The trust's DPO is Holly Senior and is contactable via:

Email: holly.senior@sharemat.co.uk

Telephone: 01484 868777

6.3 Headteachers/Principals

The headteachers/principals act as the representative of the data controller on a day-to-day basis and are responsible for ensuring that their school is compliant with data protection laws. They will delegate duties throughout the school to ensure correct processes and procedures are undertaken to meet the requirements of compliance.

6.4 All staff

Staff members are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent to process personal data
  - If there has been a data breach
  - If there has been a suspected/and or/near miss data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties
- If they would like training or awareness sessions arranged for themselves or colleagues

The trust ensures that all staff, including contract, temporary, third party and supply staff are made aware of its expectations in terms of data protection.

All staff across the trust work in a 'data safe' culture and are made aware that their actions in relation to personal data must be carried out in such a way to protect a data subject's personal data.

7. Data protection principles

GDPR is based on data protection principles that the trust must comply with. The principles are in place to protect the rights of a data subject.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

8. Rights of a Data Subject

GDPR legislation was implemented to give data subjects better security over their personal data. Data subjects are entitled to the right to:

- Be informed
- Rectification
- Erasure
- Restrict processing
- Access
- Data portability
- Object
- Object to automated decision making and profiling

The trust ensures that all processes and procedures that it undertakes are done with data subject rights in mind.

9. Collecting personal data

Upon collecting any form of personal data, the trust must assess whether it has a lawful basis for doing so. Where possible it will rely on legitimate interest, consent or public interest for processing.

9.1 **Lawfulness, fairness and transparency**

Personal data must only be processed if at least one of the six '**lawful bases'** (legal reasons) for doing so is in place:

- to fulfil a contract with an individual, or an individual has asked the trust to take specific steps before entering into a contract
- to comply with a legal obligation
- to ensure the vital interests of an individual e.g. to protect someone's life
- to perform a task in the public interest, and carry out its official functions
- for the legitimate interests of the trust or a third party (provided the individual's rights and freedoms are not overridden)
- an individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, the trust will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Parental consent for processing data will be obtained for all students under the age of 13 (except for online counselling and preventive services).

The first time we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. Where possible we will give data subjects the opportunity to 'opt in' when asking for consent rather than 'opt out'.

9.2 **Limitation, minimisation and accuracy**

The trust will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained clearly to the individuals concerned when their data is first collected.

If personal data is to be used for reasons other than those given when the data was obtained, the trust will inform the individuals concerned beforehand, and seek appropriate consent.

Staff must only process personal data where it is necessary in order to do their jobs. Staff members requiring access to personal data should contact the DPO who will carry out an assessment into the lawfulness of the request and grant or decline permission as appropriate.

At the point the personal data is no longer required, it will be deleted or anonymised. This will be done in accordance with the trust's record retention schedule (Information Records Management for Schools - IRMS). It is the responsibility of each school to maintain all records and ensure that personal data is only being held for as long as necessary.

10. Sharing personal data

The trust will not normally share personal data with anyone. It follows a rigorous procedure to assess whether personal data should be shared with a third party, including whether the other party/organisation has the correct safeguards in place to protect the data, and this is overseen by the DPO.

When it is determined that the trust will share personal data with a third party, a 'Data Sharing Agreement' is signed by both parties to protect the rights of the data subject.

Circumstances in which data may be shared include:

- an issue with a student or parent/carer that puts the safety of staff at risk
- liaising with other agencies – the data subject's consent will be obtained first
- to allow suppliers and contractors to provide services to staff and students, such as IT companies. In this instance the trust will:
    - only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
    - carry out a DPIA to assess the risk involved, as well as assessing if there are any other lower risk options available
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data
    - only share data that the supplier or contractor requires to carry out their service

The trust will also share personal data with law enforcement agencies and government bodies where it is legally required to do so, including (but not restricted to):

- the prevention or detection of crime and/or fraud
- the apprehension or prosecution of offenders
- the assessment or collection of tax owed to HMRC
- in connection with legal proceedings
- where the disclosure is required to satisfy safeguarding obligations
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects students or staff.

10.1 Post Brexit

Post Brexit, the trust will follow the steps below to continue sharing and receiving personal data lawfully:

- carry out risk reviews
- obtain legal advice if there is any uncertainty
- comply effectively with GDPR

- use the ICO free web resources to determine what changes, if any, it may need to make

There are two sets of rules to consider:

1. UK rules on transferring data outwards from the UK to the EU (including the EEA) and the rest of the world
2. the impact of EU transfer rules on those sending personal data from outside the UK (including from the EEA) into the UK

In both cases, the trust can transfer personal data if it is covered by an adequacy decision, an appropriate safeguard or an exception.

Sharing data with the EU, Iceland, Liechtenstein and Norway

The trust should contact anyone it shares personal data with within the EU, Iceland, Liechtenstein or Norway and explain that it can still share personal data lawfully with them now that the UK has left the EU.

Receiving data from the EU, Iceland, Liechtenstein and Norway

The trust should identify where it receives data from the EU, Iceland, Liechtenstein, or Norway, and determine:

- who the data controllers and processors are
- where the data is stored

Contracts: new and existing

The trust must ensure that contracts, which include the processing of personal data in the EU, provide the additional safeguards required, and where appropriate, standard contractual clauses (SCCs).
This includes where data is being transferred from a data controller within the EU, Iceland, Liechtenstein and Norway to a UK data controller, or a UK data processor. This applies to existing contracts and new contracts to be put in place.

The trust will use the ICO's interactive tool to determine what contract changes, if any, it may need to make.

11. Subject Access Requests and other rights of individuals

Individuals have a right to make a 'subject access request' to gain access to personal information that the trust holds about them. This can be done by submitting a SAR form (either via email or via post) to a specific school or to the trust. SHARE MAT has a responsibility to:

- acknowledge that the SAR has been received
- confirm that the personal data is being processed
- provide a copy of the data (where hard copy access is not viable; data subjects are invited to view their personal data)
- explain the purpose of the data processing
- share the categories of personal data concerned

- divulge who has access to the data (currently, previously and in the future, where possible) and who it has been, or will be, shared with
- identify how long the data will be stored for (in keeping with retention guidelines) and when it will be erased
- explain whether any automated decision-making is being applied to the data, and what the significance and consequences of this might be for the individual

Template forms for a 'SAR' can be found on the trust's website and should be addressed to the DPO.

Staff in receipt of a subject access request must immediately forward it to the DPO.

11.1 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our trust may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis. All decisions will be recorded by the DPO.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our trust may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis. All decisions will be recorded by the DPO.

11.2 Responding to subject access requests

When responding to requests, the trust:

- may ask the individual to provide two forms of identification
- may contact the individual via phone to confirm the request was made by them (this is an authentication process)
- will respond without delay and within one month of acknowledging the request (in accordance with GDPR legislation)
- will provide the information free of charge (SAR's may be subject to an administrative fee if it is deemed 'large scale processing')
- may ask for a time period extension (the data subject will be informed within one month of the SAR being acknowledged)

The trust will not disclose information if it:

- contains personal data on another data subject
- conflicts with an ongoing legal case
- may cause serious harm to the physical or mental health of the student or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the trust may refuse to act on it, or charge a reasonable fee to cover administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information or similar/ associated information. The DPO will assess 'unfounded' and 'excessive' requests and manage the process with the data subject.

When the trust refuses a request, it will inform the individual of the reason why, and advise them that they have the right to complain to the ICO.

11.3 Other data protection rights of the individual

Individuals also have the right to:

- withdraw their consent to processing at any time
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

12. Parental requests to see the educational record

Educational records in respect of an individual child will be provided to parents/ carers upon request. A charge may be made to cover the cost of the necessary administration.

13. Biometric recognition systems

NB. In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where the trust uses students' biometric data as part of an automated biometric recognition system (for example, the use of finger prints for cashless catering), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place. The trust will obtain written consent from at least one parent or carer before taking biometric data from the student and processing it.

Parents/carers and students/staff have the right to choose not to use the school's biometric system(s). In this case an alternative means of accessing the relevant services will be provided. For example, students/staff may use a PIN at the point of sale.

Parents/carers and students/staff can object to participation in the trust's biometric recognition system(s), or withdraw consent, at any time, and if so, the trust will make sure that any relevant data already captured is correctly erased and no longer processed.

14. CCTV

CCTV is in operation in various locations around the trust sites. The trust will adhere to the ICO's code of practice and associated legislation for the use of CCTV.

More information on the use of CCTV across the trust can be found in the 'CCTV Policy' available on the website.

15. Photographs and videos

As part of school activities, the trust may take photographs and record images of individuals within its schools.

The trust will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. A clear explanation as to how the photograph and/or video will be used will be given to both the parent/carer and student. NB. Students aged over 18 may give their own consent.

The trust may use photographs and videos for communication, marketing and promotional materials, including, but not restricted to the following:

- within a school, for example on a notice board, school magazine, brochure or newsletter
- outside of a school such as the local newspaper
- online, for example the school's website
- social media (such as twitter)

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further. Records will be amended to note that consent has been withdrawn for the child in question so that no further photographs will be used.

Photographs and videos used in this way will not be accompanied with any other personal information about the student, to ensure they cannot be identified. This protects the child and ensures total animosity.

Further information about the use of photographs and videos is available in the trust's 'Safeguarding Policy' which can be found on the website.

16. Data protection by design and default

The trust will put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- only processing personal data that is necessary for a specific purpose, and always in line with the data protection principles set out in relevant data protection law
- completing DPIA's where the trust's processing of personal data presents a medium/high risk to rights and freedoms of individuals, and when introducing new technologies
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters
- regularly conducting reviews and audits to test the privacy measures and ensure compliance
- maintaining records of the processing activities

17. Data security and storage of records

The trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, accidental or unlawful loss and destruction or damage.

In particular, (but not restricted to):

- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- papers containing confidential personal data must not be left on office/classroom desks, staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- where personal information needs to be taken off site, staff must sign it in and out from the school office
- passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices
- staff and students are reminded to change their passwords at regular intervals

- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- staff, students or governors/directors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the trust's ICT policy)
- where personal data is to be shared with a third party, the trust carries out due diligence and takes reasonable steps to ensure it is stored securely and adequately protected

18. Disposal of personal data

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely if it is not possible to rectify or update it.

For example, the trust will shred or incinerate paper-based records, and overwrite or delete electronic files. It may also use a third party to safely dispose of records on its behalf. In this case, the trust will require the third party to provide a sufficient guarantee that it complies with data protection law.

19. Personal data breaches

The trust aims to ensure that all the personal data it holds is protected to the highest possible standard. It is aware that data breaches may occur in any one of its schools, therefore a thorough data breach action plan will be implemented to manage the situation if it occurs.

Suspected data breaches and near misses also follow the same process listed below:

Step 1- Contain the breach
Step 2- Alert the DPO
Step 3- Investigate the breach
Step 4- Decide if breach requires escalating
Step 5- Report
Step 6- Implement better practise
Step 7- Close the breach and monitor for reoccurrences
When appropriate, the trust will report the data breach to the ICO within 72 hours.

The DPO will assess if a data breach needs reporting to the ICO by using the ICO's data breach reporting guidelines available on their website. All data breaches will be recorded and logged on the trust's internal shared drive with limited access and in a locked central services cabinet.

For more information on our data breach process please see our 'Data Breach Policy' and 'Data Breach Report Template'.

20. Training

The trust aims to ensure that all staff are effectively trained and educated on GDPR and data protection. This is achieved by running annual training sessions, online training courses, drop-in sessions, newsletters and legislation update briefings.
Advanced GDPR training is offered to staff in positions of authority/responsibility such as governors/directors and Headteachers.

21. Links with other policies and documents

The trust has a full suite of policies in place to ensure data protection compliance, as follows:

- Privacy Notice (external, general)
- Privacy Notice (parents and carers)
- Privacy Notice (students)
- Privacy Notice (internal, staff)
- Record of Processing Activity Policy
- Data Breach Policy
- Data Breach Report
- Data Breach Log
- Records Management and Retention Policy
- Staff Training Policy
- Subject Access Request Policy
- Subject Access Request Templates
- Data Protection Impact Assessment Policy
- Data Protection Impact Assessment Template
- CCTV Policy
- ICT Policy
- Freedom of Information Policy
- Safeguarding Policy

22. Contact us

Questions regarding data protection, information within this policy or general concerns about data should be addressed to the DPO:

Holly Senior - Data Protection Officer and Compliance Officer

holly.senior@sharemat.co.uk

01484 868777

23. Complaints

Complaints should be addressed in the first instance to the DPO and escalated to the Information Commissioners Office if necessary:

www.ico.org.uk/contact-us