SHARE
MULTI-ACADEMY TRUST

GENERAL DATA PROTECTION REGULATION POLICY

GDPR POLICY TO BE USED BY ALL SCHOOLS IN THE TRUST

Version	2.0
Name of policy writer	Debbie Howard
Last updated	September 2019
Review date	September 2020
Approved by Directors	03 October 2019
ICO Reg Number	Z2844414

Record of Alterations
Version 1.0 Original
Version 2.0 Amendments

CONTENTS

1. Overview

SHARE MAT aim to ensure that all processes and procedures that we deliver are in line with all relevant forms of data protection legislation. As part of the General Data Protection Regulation, SHARE MAT are required by law to outline everything that we aim to do in response to the GDPR. SHARE MAT believe that we have met the requirements of this within this policy.

As well as our 'GDPR Policy' SHARE MAT also have a full policy suite accessible on our SHARE MAT website, each of the school's websites, on our internal shared drives and in the Admin Managers 'Toolkit'. We make all of our policies accessible to help educate staff on the correct processes and procedures to follow for the whole trust to be GDPR compliant, whilst providing the correct information to staff, pupils, parents and the general public.

2. Purpose

The purpose of this policy is to inform data subjects on SHARE MAT's processes and procedures that we carry out in accordance to the GDPR. Our trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, but not exclusive to, paper or 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. This policy 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.

In addition, this policy also complies with the Trust's funding agreements and articles of association.

This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

This policy also complies with our funding agreement and articles of association.

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 therefor 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'	A '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 ICO (Information Commissioners Office) and the legal authority whom mange GDPR and Data Protection.

A DPIA (Data Protection Impact Assessment)	A DPIA is a process that we carry out in order to assess if we are 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 their personal data that is held on them.

5. The data controller

Our trust processes personal data relating to parents, pupils, staff, governors, visitors and others. As we are processing personal data, under the GDPR that makes SHARE MAT (and all of the schools within the trust) 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 our trust, and to external organisations or individuals working on our 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 our trust complies with all relevant data protection obligations. The governing board are educated to a sufficient level to advise on GDPR and Data Protection matters that may arise within each school and across the trust.

6.2 Data protection officer

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

They 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.

SHARE MAT outlines all duties of the DPO within its 'Data Protection Officer Policy' which can be found on SHARE MAT website or can be accessed by contacting the DPO.

Our DPO is Holly Senior and is contactable via:

Email: holly.senior@sharemat.org

Telephone: 01484 868777

6.3 Head teachers/Principals

The head teachers/principals act as the representative of the data controller on a day-to-day basis.

The Head Teachers/ Principles of each school are responsible for ensuring that their school are compliant to data protection laws.

Head Teachers/ Principles 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 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

SHARE MAT ensure that all staff, including contract, temporary, third party and supply staff are given the correct information from the offset on our expectations of staff in terms of data protection.

All staff across the trust work in a 'data safe' culture. We implement this mind-set to help make all staff aware that any action that they do that comes into contact with personal data is done in such a way to protect a data subject's personal data.

7. Data protection principles

The GDPR is based on data protection principles that our trust must comply with. The principles are put in place to ensure that everything that we do protects 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

This policy sets out how the trust aims to comply with these principles.

8. Rights of a Data Subject

The GDPR legislation was implemented to give data subjects better security over their personal data. The GDPR outlines that data subjects are entitled to:

8.1. The right to be informed

8.2. The right to rectification

8.3. The right to erasure

8.4. The right to restrict processing

8.5. The right to access

8.6. The right to data portability

8.7. The right to object

8.8. The right to object to automated decision making and profiling

SHARE MAT ensure that all processes and procedures that we undertake are done with data subjects rights in mind.

9. Collecting personal data

SHARE MAT assess when we collect any form of personal data if we have a lawful basis for doing so. Where possible we will always rely on: legitimate interest, consent or public interest for processing.

9.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 '**lawful bases'** (legal reasons) to do so under data protection law:

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

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first 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 as oppose to an 'opt out' (soft opt in) option.

9.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data in a clear and concise manner.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. If staff require access to personal data, they will contact the DPO and an assessment into the lawfulness of this will be undertaken. If the DPO is happy for access to be granted they will sign this off.

When we no longer need the personal data they hold, we will ensure it is deleted or anonymised. This will be done in accordance with the trust's record retention schedule (IRMS Records Management for Schools). 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

SHARE MAT do not normally share personal data with anyone. SHARE MAT follow a rigorous procedure when assessing if personal data should be shared with a third party. This will be overseen and conducted by the DPO.

When we do choose to share personal data with a third party, a 'Data Sharing Agreement' will be used to protect the rights of the data subject, as well as assessing if that organisation has the correct safeguards in place to protect this data.

We will not normally share personal data with anyone else, but may do so where (but not restricted to):

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will contact the data subject and ask for consent before doing so
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Carry out a DPIA to assess the risk of establishing this action, 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 we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are 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 our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law of the EU, NOT the data protection laws of the country being transferred to.

SHARE MAT believes in upholding the best security processes for data protection. If any organisation wishing to obtain personal data that we hold is NOT an EU Member State (or part of the EEA) we will insist they uphold the same data protection practise that would be required by all companies operating in the EU. If an organisation does not have sufficient data protection safeguards we will restrict processing.

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 have a responsibility to provide:

- Acknowledgement that their SAR has been received
- Confirmation that their personal data is being processed
- Access to a copy of the data (where hard copy access is not viable, data subjects are invited to view their personal data)
- The purposes of the data processing
- The categories of personal data concerned
- Who has access to their data (currently, previously and in the future, where possible)
- Who the data has been, or will be, shared with
- How long the data will be stored for along with retention guidelines on how and when this will be erased
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

When submitting a 'SAR' they should be addressed to the DPO of the trust and filled in using one of SHARE MAT's SAR templates available on the website (information on this can be found on the 'contact us' section of this policy):

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they 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 12 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 pupils at our trust may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. All decisions will be logged by the DPO.

Children aged 12 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 pupils at our trust may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis. All decisions will be logged by the DPO.

11.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 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 1 month of acknowledging the request (as per the new guidance of the GDPR legislation)
- Will provide the information free of charge (where applicable, SAR's may be subject to an administrative fee when deemed 'large scale processing')
- May ask for an extension on the SAR (the data subject will be informed within one month of the SAR being acknowledged as well as informed as to why the SAR is being extended)

We will not disclose information if it:

- Contains personal data on another data subject
- Conflicts with an ongoing legal case
- Might cause serious harm to the physical or mental health of the pupil 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, we may refuse to act on it, or charge a reasonable fee which takes into account 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/ associating information. The DPO will assess 'excessive use' and manage the process with the data subject.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

11.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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.

For further information on SAR's please see out 'Subject Access Request Policy'.

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

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), 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 get written consent from at least one parent or carer before we take any biometric data from their child and first process it. SHARE MAT will use an 'opt in' system for collecting consent instead of an 'opt out' (soft oft in) process.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils may use a PIN at the point of sale.

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

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

14. CCTV

We use CCTV in various locations around the trust sites to ensure they remain safe. SHARE MAT will ensure we adhere to the ICO's code of practice for the use of CCTV along with all other forms of associating legislation.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use and the contact details of monitoring management.

SHARE MAT assess the placement of CCTV to prevent capturing 'private information'. We use a risk assessment process to determine if the placement of a CCTV camera is capturing data that breaks the rights of a data subject.

For more information on CCTV across the trust please see our 'CCTV Policy' available on our website.

Any enquiries about the CCTV system should be directed to the Facilities Manager or the Compliance Officer.

15. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.

For our primary schools, we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

For our secondary schools, we will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental

consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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

- Within a school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of a school by external agencies such as the school photographer, newspapers, campaigns
- Online for our school's website or social media pages
- Social media (such as twitter)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. We will also keep on record that consent has been withdrawn for that child so no further photographs will be used.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. We do this to protect the child and ensure total animosity.

Please see our 'Safeguarding Policy' available on our website for more information on our use of photographs and videos.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our 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 each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- 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 (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

17. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, 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 and classroom desks, on 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 pupils 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, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected, please refer to section 10, 'Sharing Personal Data'

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, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Personal data breaches

SHARE MAT aim to ensure that all personal data that we hold is protected to the highest possible standard. We are aware that data breaches may occur in any of our

schools, therefor we implement a thorough data breach actions plan to manage if/ when a data breach 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, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

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 in a data breach tracking format stored on our 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

SHARE MAT aim to ensure that all staff across the trust are effectively trained and educated on GDPR and data protection. We do this be running annual training sessions for staff, online training courses, drop-in sessions and newsletters and legislation updates.

As well as general GDPR training, specialist staff such as Governors and Head Teachers are offered the opportunity to attend advanced GDPR training delivered by the trust's DPO.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the trust's processes make it necessary.

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our trust's practice. Otherwise, or from then on, this policy

will be reviewed every 2 years and shared with the full governing board for approval and with each school for distribution and display.

22. Links with other policies and documents

SHARE MAT have a full policy suite in place across the trust to ensure data protection compliance. Please see a comprehensive list of all of our policies below:

- 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
- IT Policy
- Freedom of Information Policy
- Safeguarding Policy

23. Contact us

If you have any questions regarding data protection, information within this policy or general concerns surrounding your data please feel free to contact our DPO:

Holly Senior

Data Protection Officer and Compliance Officer

holly.senior@sharemat.org

01484 868777

24. Complaints

If you feel that your data is not being handled correctly and you have not had an acceptable response from our DPO you are entitled to raise this issue with the supervisory authority, The Information Commissioners Office.

To contact the ICO please visit:

www.ico.org.uk/contact-us