GENERAL DATA PROTECTION REGULATION POLICY & PROCEDURE

To be used by all academies in the Trust

MAT version	4.0
Name of Policy Writer	Natalie McSheffrey
Date of last review	n/a
Date of next review	February 2026
Approved by Trustees	6th February 2025

Schedule of amendments:

V4 – NEW version updated inline with DfE legislation updates

Contents

1. **Data Protection Overview** 2
2. **Updates to the Data Protection and Digital Information Bill** 5
3. **Data processing** 5
4. **Responsibilities** 6
5. **Role of the data protection officer (DPO)** 7
6. **Data protection policies and procedures** 8
7. **Processing activities** 8
8. **Sharing personal data** 10
9. **Dealing with subject access requests (SARs)** 13
10. **Handling other information rights requests** 16
11. **Data retention** 16
12. **Managing breaches of data** 17
13. **Generative Artificial intelligence (AI) and data protection in schools** 19
14. **Contact Us** 20
15. **Complaints** 20

1. Data Protection Overview

Data protection law

SHARE MAT aims to ensure that all its processes and procedures are in line with relevant data protection legislation, set primarily by:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018 (DPA)

This policy:

- is based on the guidelines set out by the Information Commissioner's Office (ICO) and The UK General Data Protection Regulation and Data Protection Act 2018 legislations.
- complies with the trust's funding agreements and articles of association.
- meets the requirements of the Protection of Freedoms Act 2012 and the Freedom of Information Act (2000) 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.

Data Protection principles

The trust adheres to the UK GDPR 7 key principles when processing personal data. Those principles are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability.

Personal data

Personal data is information that relates to an identified or identifiable living individual. Examples of personal data in our trust include:

- identity details (for example, a name, title or role)
- contact details (for example, an address or a telephone number)
- information about pupil behaviour and attendance
- assessment and exam results
- staff recruitment information
- staff contracts
- staff development reviews
- staff and pupil references.

Special Category Data

Special category data is personal data that's considered more sensitive and given greater protection in law. Examples of special category data within SHARE MAT includes:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- genetic information
- biometric information (for example, a fingerprint)
- health matters (for example, medical information)
- sexual matters or sexual orientation.
- a safeguarding matter
- pupils in receipt of pupil premium
- pupils with special educational needs and disability (SEND)
- children in need (CIN)
- children looked after by a local authority (CLA).

Criminal offence data

Criminal offence data is personal data that is treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures.

Criminal offence data includes:

- the alleged committing of an offence
- the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing.

SHARE MAT processes criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means the school is processing criminal offence data. This applies even if the check has not revealed any conviction.

Data Subjects

SHARE MAT collect, store and use personal data about a variety of individuals. In this context, those individuals are known as data subjects.

Data subjects include:

- pupils and former pupils
- parents and carers
- employees and non-employed staff
- governors and trustees
- local-authority personnel
- volunteers, visitors and applicants.

Data assets

Personal data is held by our central services and academies in several forms. These are collectively known as its data assets.

Data assets comprise:

- data items – single pieces of information
- data item groups – data items about the same process
- data sets – collections of related data that can be manipulated as a unit by a computer
- systems – administrative software
- system groups – the larger systems housing administrative software.

Personal data breaches

A data breach is a security incident that results in personal data the trust holds being:

- lost or stolen
- destroyed without consent
- changed without consent
- accessed by someone without permission.

Data breaches can be deliberate or accidental.

2. Updates to the Data Protection and Digital Information Bill

The trust is guided by the DfE regarding the planned changes to legislation in the Data Protection and Digital Information Bill. This policy will be updated to reflect any changes that may occur.

The bill makes changes to the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications (EC Directive) Regulations 2003

3. Data processing

Under data protection legislation, there are a number of justifications that permit personal data to be processed. SHARE MAT will ensure that they apply at least 1 of the following 6 lawful bases before personal data is permitted to be processed, identifying the most appropriate.

The lawful bases are:

- **consent** – where this basis is the most appropriate and we are able to give the individual concerned a real choice in our use of their data
- **contract** – where our use of the data is necessary for a contract the school has or will have with the individual concerned
- **legal obligation** – where our use of the data is necessary to permit the trust to comply with the law
- **vital interests** – where our use of the data is necessary to protect an individual's life
- **public interest** – where our use of the data is necessary to permit the trust to carry out a task in the public interest or its official functions, and that task or function has a clear basis in law
- **legitimate interests** – where our use of the data is necessary for the trust's or a third party's legitimate interests (unless there's a good reason to protect the individual's personal data that overrides those legitimate interests).

Special category data: the justifications

Under UK GDPR, there are 10 additional conditions for processing special category data. SHARE MAT will apply at least one lawful basis and one condition – which does not have to be linked to the lawful basis. The conditions are:

- **explicit consent** – the accessing or processing of this personal data has the written consent of the individual concerned
- **employment, social security or social protection** – it's necessary for one of these 3 stated purposes and authorised by law
- **vital interests** – it's necessary to protect an individual's life
- **not-for-profit body** – it's necessary for the legitimate internal-only purposes of a membership body with a political, philosophical, religious or trade-union aim
- **manifestly made public** – it relates to personal data the individual has themselves deliberately made public
- **legal claims or judicial acts** – it's necessary for a legal case or required by a court of law
- **substantial public interest** – there's a relevant basis in UK law and one of 23 specific public interest conditions has been met

- **health or social care** – it's necessary for the provision of healthcare or treatment, or of social care, and there's a basis in law
- **public health** – it's necessary for reasons of public interest, and there's a basis in law
- **archiving, research and statistics** – it's necessary for reasons of public interest, and there's a basis in law

Any further actions which might be necessary will be taken in line with the Data Protection Act 2018 (DPA), Schedule 1, Parts 1 and 2.

Criminal offence data: the justifications

One of the 6 lawful bases will be applied by SHARE MAT before processing criminal offence data and it will be covered by one of the conditions described in Schedule 1 of the DPA.

If the lawful basis of **consent** applies, the condition for processing any special category data within would be **explicit consent** - that is, consent that has been confirmed in a written statement.

UK GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. For consent to be considered 'freely given', SHARE MAT will ensure that an individual will not suffer any detriment if they refuse to give it.

4. Responsibilities

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

Everyone in SHARE MAT is responsible for protecting personal data. There are some key roles and responsibilities for data protection compliance.

The data controller

SHARE Multi-Academy Trust is the data controller and is registered as such with the Information Commissioner's Office. This means it is responsible under the Data Protection Act 2018 for protecting data in every situation where it decides:

- whose information to collect
- what types of data it needs
- why it needs it
- whether the information can be shared with a third party
- when and where data subjects' rights apply
- for how long to keep the data

Governors and trustees

The responsibility and accountability for compliance sits with the Trust Board. Governors and Trustees check that schools and the central team:

- monitor their data protection performance
- support the data protection officer
- have good network security infrastructure to keep personal data protected
- have a business continuity plan in place that includes cyber security.

Senior leaders

Senior leaders are accountable for:

- deciding how the school/trust uses technology and maintains its security
- deciding what data is shared and how
- setting policies for the use of data and technology
- understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate
- assuring governors and trustees that the trust has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive training on data protection every 2 years to include data breach reporting processes and the escalation of information rights requests.

All staff

All staff, including the Trust Board and Governors are trained via an external accredited provider and are aware of what:

- personal data is
- 'processing' means
- their duties are in handling personal information
- the processes are for using personal information
- is permitted usage of that data
- the risks are if data gets into the wrong hands
- their responsibilities are when recognising and responding to a personal data breach
- the process is for recognising and escalating information rights requests.

Staff who collect, store, create or view personal data are responsible for:

- making sure they have a legitimate need to process the data
- checking that any data they store is needed to carry out necessary tasks
- identifying any risks
- understanding the governance arrangements that oversee the management of risks.

Staff are responsible for making sure that pupils using personal data for projects or coursework do so appropriately. This includes being compliant when storing data.

5. Role of the data protection officer (DPO)

The trust's DPO is Jayne Newson and is contactable via:

Email: jayne.newson@sharemat.co.uk

Telephone: 08452 415175

The DPO within SHARE MAT helps to ensure the trust are compliant with data protection laws.

Data protection officer's responsibilities

The SHARE MAT data protection officer is responsible for:

- advising leaders and staff about their data obligations
    - monitoring compliance
    - conducting regular data audits

- developing and updating data protection policies and procedures
- monitoring who has access to personal data
- advising when data protection impact assessments are needed
- answering data protection enquiries from staff, parents and pupils
- making sure privacy notices are regularly reviewed and updated
- supporting and advising staff who have data protection queries
- communicating with the Information Commissioner's Office (ICO)
- reporting to the trust board and governing bodies about data protection
- advising the trust board and governing bodies on data protection risks
- advising on and co-ordinating responses to information rights requests
- making sure all assets containing personal data are appropriately managed and secure.

6. Data protection policies and procedures

Under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), the trust has to:

- comply with the legislation
- demonstrate that they're complying.

Statutory policies

SHARE MAT takes the legal requirement very seriously and has data protection policies and procedures in place which are reviewed and updated annually, along with other associated policies and documentation.

7. Processing activities

Record of processing activities

By taking steps 1-10 identified below, SHARE MAT capture all the important information about the trust's data processing activities, to include mandatory information and any additional information deemed necessary to evidence compliance with accountability principles.

Step 1: identify personal data assets

Step 2: list personal data assets

Step 3: source of personal data

Step 4: Category of personal data

Step 5: Data controller or data processor

Step 6: Access and use

Step 7: Data retention and destruction

Step 8: Consent, rights and subject access requests

Step 9: Security and personal data breaches

Step 10: Automated decision-making.

Data protection impact assessment (DPIA)

In line with UK GDPR, SHARE MAT prepare a DPIA whenever the processing of personal data is likely to result in a 'high risk to the rights and freedoms' of individuals. The DPIA will:

- identify, manage and mitigate data protection risks
- fix problems at an early stage, minimising those risks
- consider and mitigate risks to individuals' privacy
- ensure individuals' expectations of privacy obligations are being met - for example, by the provision of privacy notices
- provide individuals with reassurance
- demonstrate both accountability and compliance with data protection law
- avoid reputational damage to our trust

SHARE MAT will consider and document carrying out a DPIA of personal data collected:

- about vulnerable data subjects, including:
- children (because of their age)
- employees (because the power imbalance means they cannot easily consent or object to the processing of their data by an employer)
- more vulnerable sectors of the population (who need special protection)
- by innovative technologies, such as:
- biometrics
- internet of things applications
- safeguarding equipment, such as CCTV.

Recording of the risks

Should the DPIA identify a high risk that cannot be minimised by control measures, the DPO will seek advice from the ICO before any personal data is processed.

Reassessment of the impact

DPIAs will be kept under regular review and updated should anything changes occur.

Privacy notices

SHARE MAT ensure that under UK GDPR and the Data Protection Act 2018, privacy notices are freely available to those whose personal data it handles.

A SHARE MAT privacy notice explains:

- why we need to collect personal data
- what we plan to do with it
- how long we will keep it
- whether we will be sharing it with any other organisation.

SHARE MAT privacy notices are clear and accessible to data subjects at all times and explain what makes it lawful for the trust to use personal data, including any data that may be regarded as sensitive.

Privacy notices are reviewed annually by the DPO or whenever a significant change to how the trust process personal data is made.

Parents, pupils, staff, visitors, governors and trustees, who are the data subjects, are notified in the case of any significant changes to our privacy notices or if the way we use their personal data changes.

Data subjects' rights

Data subjects' rights over the use of their personal data are key to a privacy notice. They are:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision-making and profiling

SHARE MAT privacy notices include:

- what personal data is being processed
- why their personal data is being processed
- on what lawful basis their personal data is being processed
- with whom their personal data will be shared and why
- how and for how long their personal data will be stored
- how they can exercise their rights over their personal data
- whom to contact if they have any questions or concerns, including your data protection officer and the ICO.

Personal information shared with DfE

DfE collects personal information from SHARE MAT via various statutory data collections. Each data collection or census guide contains the legislation detailing the lawful basis for collection.

This data is used for many purposes, including to inform funding, monitor education policy and school accountability, and to support research.

SHARE MAT privacy notices include what personal data is shared with DfE.

Cyber security and safeguarding

SHARE MAT take all necessary steps to ensure critical data is protected from cyber-attacks and unauthorised access. Further details are available in the SHARE MAT ICT Policy & Procedure.

8. Sharing personal data

To keep children and young people safe, SHARE MAT only share information appropriately to protect them.

Safeguarding and the sharing of data

To keep children safe and make sure they get the support they need, SHARE MAT may share information with other schools, local authorities or other children's services. It's not usually necessary for us to ask for consent to share personal information for the purposes of safeguarding a child.

Should leaders decide if personal data needs to be shared, they will record the following:

- who they are sharing the information with
    - why they are sharing the data
    - whether they have consent from the pupil, parent or carer.

The trust will always refer to "Working Together to Safeguard Children" and the safeguarding section of "Keeping Children Safe in Education" to ensure we are adequately safeguarding the children in our trust.

Before we share any data, we will:

- consider all the legal implications
- check if you need permission to share the data
- confirm who needs the data, what data is needed and what they'll use it for
- make sure we have the ability to share the specified data securely
- check that the actions cannot be completed or verified without the data.

SHARE MAT also have a statutory requirement to share personal data about our pupils with the DfE through the school census. We do not need to get consent from pupils, parents or carers to share this data but will share information about the data we share in our privacy notices.

We may also need to share personal data about SHARE MAT staff and governance volunteers with the local authority.

If a pupil moves to another school, records are securely transferred to the new school.

If we are organising a school trip with another school, we will share data with them to confirm which pupils are going. We may also need to share details such as dietary requirements or medical information to make sure pupils are safe.

When consent is not appropriate

Before sharing any personal data, SHARE MAT will identify the lawful basis. This may be consent from the individual. There may be some circumstances where it may not be appropriate to ask for consent, however. For example:

- if the individual cannot give consent
- it's not reasonable to ask for consent
- when there's a safeguarding concern.

Obtaining a pupil's consent

SHARE MAT will usually get the pupil's consent to share their data if they're aged 13 or over. A clear explanation will be provided to the pupil why we are seeking consent. If they are under 13, we will seek consent from whomever holds parental responsibility for the child.

How to get consent

SHARE MAT will ensure the individual agrees to share their personal data and understands what they're agreeing to. We will record:

- the consent
- when we obtained the consent
- how we obtained the consent
- what personal information we are sharing
- why we are sharing it
- who we are sharing it with and what they will use it for
- how we will share their information
- the process for withdrawing consent.

Biometric data

SHARE MAT comply with the requirements of the Protection of Freedoms Act 2012 with regards to using pupils' biometric data as part of an automated biometric recognition system, such as using fingerprints to receive school meals instead of paying with cash.

We will take the following steps.

1. In accordance with the child's age or capacity, get written consent from at least one parent or carer before we take and process any biometric data from the child.
2. Provide an alternative means to access the relevant services for any pupil from whom we do not have consent. For example, pupils must be able to pay for school meals using cash at each transaction, if they wish.
3. Delete any relevant data already captured, if a parent or carer withdraws their consent.

If a pupil does not want their biometric data processed, we will not process it even if the parent or carer has given consent. This is required by law.

We will also obtain consent from any staff members using the school's biometric system. Staff can withdraw their consent at any time and we will then delete any relevant data already captured.

Taking and using photos in school

Photos are used in school for many different reasons. SHARE MAT will always identify the lawful basis for each different use of a photograph.

From time to time, we may use photos in printed materials such as a prospectus or marketing materials under the lawful basis of legitimate interest. However, we will always provide pupils, parents or carers with an opportunity to object before we go to print. Likewise, we will always obtain consent to share photos on trust social media channels or elsewhere online and seek specific consent to use a pupil's name. When we ask for consent, we will make it clear for how long we will use the photograph.

Photos used in identity management systems may be essential for performing the public task of the school, but we will delete them once a child is no longer a pupil at the school.

Publishing exam results

UK GDPR does not stop schools from publishing exam results online or in the local press. SHARE MAT do not need to get consent from pupils, parents or carers to publish exam results. However, we will tell pupils where and how their results will be published beforehand. This will allow an opportunity for the removal of their results from the list should they wish to.

Immunisation Programmes

SHARE MAT will need to provide data to support immunisation programmes in our schools. This includes:

- sharing information leaflets and consent forms with parents or carers
- providing a list of eligible children and young people, and parent/carer contact details to the School Age Immunisation Service (SAIS) team.

Sharing these contact details does not mean that a vaccine will be given. A parent or carer will need to give their consent for a vaccine to be given to their child.

There is a lawful basis for you to share information with school immunisation teams under article 6(1)(e) of UK GDPR. This states that the information can be shared if "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

This means that the school can share this information with immunisation programmes as it is in the public interest.

Sharing information with immunisation programmes is part of the exercise of a school's official authority. Schools also have a duty to support wider public health.

Data protection laws do not prevent schools from sharing personal data where it is appropriate to do so in a fair and lawful way, and in this instance it is beneficial to do so.

9. Dealing with subject access requests (SARs)

A subject access request (SAR) is a type of information rights request. A SAR lets people access a copy of the personal data the trust holds about them or someone they have parental responsibility for, or someone they have permission to act on behalf of.

Receiving a SAR

Any individual whose personal data is held by an education setting can make a SAR. Personal data is information that relates to an identified or identifiable individual.

The person making a SAR is referred to as the requester. Individuals can ask for a SAR from anyone who works within the trust and a SAR can be made in any format, i.e. verbal request, or a written request via a letter, text, or email. Once an individual has made a request, we will not ask them to change the format they made the request in. When an individual asks for their personal data, they do not have to call it a SAR, for example it may take the form of a complaint or freedom of information request.

Clarifying a SAR

Whilst we cannot ask the requester to narrow or reduce their request, we may ask for clarification of what specific information the requester is looking for. This might be helpful when the requester asks for a lot of information because they are not sure what they need.

When requesters can self-serve

If the requester already has access to the information they want to see, we will direct them to this. We will not treat this request as a SAR, provided they can access the information within one calendar month.

Checking the identity of someone submitting a SAR

In most cases when an individual makes a SAR we will need to ask for identification (ID) from them. However, in a school setting, pupils and their parents or carers are generally well-known to school staff. If we know the requester and are sure of their identity and authority, staff will not request ID and a record of why they made this decision will be made.

If the requester is asking for their own information, and staff do not know them, then they will need to provide their identification.

Adults should provide a photo ID plus another form of ID, this could be:

- their driving license or passport for the photo ID
- a utility bill or council tax bill that confirms their name and address

If the requester is asking for another individual's information, then they will need to provide the individual's ID and they will also need to provide evidence that they have the authority to act on the individual's behalf. This includes requesters such as parents and solicitors.

If the requester cannot provide the standard ID, it is the data controller's decision whether alternative identification is appropriate and a record of the decision-making process will be made.

Responding to a request from a child

Requesting a SAR is a child's right. A child can request access to information about themselves from any education setting that holds data about them. A child does not have to be a certain age to make a SAR.

If the young person is under 13 and is making their own request, SHARE MAT will consider whether they will be able to understand the response, but this will not be a barrier to supplying them with their information.

If the young person is over 13, we will treat the request the same way as if an adult made it, provided there are no issues with the child's competency.

Parents or carers can also make a SAR on behalf of a young person. If the young person is 13 or over, we will obtain consent for their personal data to be shared with their parent or carer.

If we believe the child has the maturity and understanding to request and receive the information, we will respond directly to the child, regardless of their age. If a child requests a SAR themselves, this demonstrates some maturity and understanding about their right of access their personal information.

We will not respond directly to the child if we believe they:

- do not have the maturity or competence to act independently
- have a health condition that limits their understanding
- have given consent for a representative or someone with parental responsibility to act on their behalf.

In these cases, we will contact the child and ask if they agree for their parent or carer to make the request on their behalf.

Timeframes for responding to a SAR

A full SAR response must be sent to the requester within one calendar month.

We will extend the SAR deadline if we have to wait for the requester to provide identification, authority and any clarification we might need.

If the request is complex, the response time can be extended by up to a further 2 calendar months, making the response deadline 3 months in total. We will, however, respond to the SAR as soon as possible within the extended period.

For complex requests, we will tell the requester the new deadline and the reason their SAR is being treated as complex, in writing, within one calendar month of the original request date.

If SHARE MAT receive a SAR on the last day of the school term, or during the school holidays, we will still respond within one calendar month.

Charging for a SAR

Whilst we will not charge a fee to complete a SAR, in some cases we may have no option but to charge for administration costs associated with completing a SAR.

Information to include in a SAR response

We will make reasonable efforts to search through all records, including:

- emails (including those in deleted or trash folders)
- documents
- spreadsheets
- databases
- record systems
- CCTV
- USB sticks or CDs
- paper records in filing systems
- instant messages.

Redacting information

SHARE MAT may need to remove some information. This process is known as redacting. We will redact personal information that identifies anyone other than the person the SAR is about. This is known as removing third party information. A SAR entitles a person to access their own personal information but does not entitle them to access full documents. Where staff or professional bodies form part of the SAR, we will not redact their name, nor will be redact the names of parents.

Individuals may ask to see CCTV images of themselves or their child. CCTV images contain personal information. Images of other people appearing in CCTV images will be redacted, for example by blurring. Further information can be found in the SHARE MAT CCTV Policy & Procedure.

Information that is no longer available

In some cases, a requester may ask for information that the trust no longer hold. We will respond by telling them the information is no longer held on record.

SAR response formats

Usually, a SAR response will be made in the same format as the request was received.

A written response is preferable, but we can provide a verbal response if the requester asks for one. We will, however, keep a written record of the response.

All responses will be submitted in a secure way.

Making sure a SAR response is accessible

We will ensure the process is as simple as possible for individuals, especially those who may need additional support to make a SAR.

Refusing to comply with a SAR

SHARE MAT may refuse to comply with a SAR if:

- a data protection exemption can be applied to all the personal information in scope of the request
- the request is manifestly unfounded or manifestly excessive

Examples of exemptions that may apply to education settings include:

- releasing the information would cause serious harm to a child
- releasing information would not be in the best interests of a child
- information relating to third parties
- legal advice sought and received from a lawyer
- information that may prejudice an investigation

Manifestly unfounded or excessive SARs

A manifestly unfounded SAR is when an individual submits multiple SARs with malicious intentions. SHARE MAT may refuse to comply with a request on these grounds but will always provide a rationale to the requester for the decision within one calendar month from the day the SAR was submitted. The requester will be given details about how to complain to the ICO or seek a judicial review.

Complaints about a SAR response

A SAR response letter will include the following information:

- organisation contact regarding the response, usually the data protection officer
- details on how to complain to the ICO
- acknowledgement of their right to seek judicial remedy
- acknowledgement of their other data protection rights such as the right to have their information deleted or changed.

If the requester is unhappy with their SAR response, they will be offered the chance for their case to be reviewed.

If the requester remains unhappy with the trust's response, they can complain to the ICO. The ICO will consider the complaint and contact the trust for further information or to provide advice as appropriate.

Recording the SAR process

SHARE MAT will keep a record of the SAR process from start to finish. Details recorded will include:

- the date the request was received
- any time the response was paused and why (for example getting identification)
- a copy of all correspondence
- information about which records and systems were searched and what was found
- any information that was redacted and the reason why
- the date we sent the response and a copy of it
- copies of any ongoing correspondence with the requester (such as confirmation of receipt, complaints)
- evidence of decision to refuse a SAR
- evidence of decision to exempt any information.

10. Handling other information rights requests

Information rights mean a person has the right to access or amend the personal data any organisation holds about them.

The most common type of information rights request is a subject access request (SAR). This is when someone requests to see the personal data an organisation holds about them.

Individuals, including children, have several information rights relating to personal data a school may hold about them.

Information rights request that someone might make include asking to:

- change inaccurate personal information you hold about them
- remove their personal information or record
- restrict the processing of their personal information
- stop processing their personal information (right to object).

SHARE MAT will accept an information rights request relating to personal data either verbally or in writing, including through social media.

Unless there's a valid reason, we will respond to any information rights request within one calendar month. If the case is complex we may extend the response deadline by an extra 2 calendar months.

Information rights requests only apply to the personal data we hold on receipt of the request.

Individuals have the right to request changes or restrictions to personal information, but our trust is not obliged to make changes to data in certain circumstances.

11. Data retention

SHARE MAT will only keep data for as long as it is required in accordance with current IRMS recommendations and in line with the Data Protection Act 2018 and UK GDPR guidance which will be checked annually.

Where we identify any information we no longer need, it will be disposed of securely.

Data retention

The SHARE MAT data retention schedule explains how long the trust need to keep information. It will set out:

- why we are holding this data
- our justification for keeping the data
- the lawful basis for processing and keeping the data
- if we will pass this data on and, if so, once passed on, if we need to keep it
- the steps we will take when we destroy any personal data
- if it is more appropriate for another organisation such as the local authority to keep the information in the long term
- if we will need the data to meet Ofsted's requirements
- whether we can delete or depersonalise some of the information.

Personal data audit

SHARE MAT carry out an audit of all the personal data it holds each year to check it is up to date and still needed. We will not keep any data longer than is necessary.

The results will be shared with school leaders, governors and trustees. They are responsible for making sure the school is compliant with the Data Protection Act 2018 and only keeps data it needs.

Depersonalising personal data

As data becomes older, there are steps SHARE MAT may take to keep data about pupils for analytical purposes. Before deleting the data completely, we may remove names and personal identifiers. This will remove some of the risks around personal data. It will also allow the trust to use it for long-term analysis of trends.

Another option is to replace the personal information with non-personal identifiers. For some records, we may only need to keep summary statistics.

Disposal of personal data

When records have reached the end of their retention period, data must be disposed of securely and confidentially. All staff are aware of the following procedures to help prevent any data breaches:

- shred paper records using a cross-cutting shredder, or get an external company to shred them
- destroy storage media and hard disks to particles no larger than 6mm
- dismantle and shred audio and video tapes

Where we use an external company to destroy records, it will:

- shred all records on-site in the presence of an employee
- be able to prove that the records have been destroyed and provide a certificate of destruction
- have trained its staff in the handling of confidential documents.

It is a requirement of The Freedom of Information Act 2000 that SHARE MAT maintain a list of records that have been destroyed and who authorised their destruction.

12. Managing breaches of data

A data breach is a security incident that has resulted in personal data being:

- lost or stolen
- destroyed without consent

- changed without consent
- accessed by someone without permission.

Data breaches can be deliberate or accidental.

Identification and investigation of a personal data breach or suspected personal data breach

UK GDPR places certain legal obligations onto organisations relating to the handling of personal data breaches.

SHARE MAT members of staff:

- are able to recognise when a personal data breach has taken place
- will check if the incident involves personal data, understand what types of personal data are involved and who the data subjects are
- know how to report it formally.

The trust data protection officer will:

- support throughout the process
- where necessary, liaise with the Information Commissioner's Office.

Take action to limit further impact

It will be a priority to establish what has happened to the personal data, who has access or might have access to it as this will affect the level of risk involved. Where possible, we will recover the data immediately. This might include:

- recalling, or asking someone to delete, an email containing personal data sent by mistake
- retracing steps or contacting reception if physical data has been lost to see if it has been handed in
- checking if you can lock or wipe a laptop, phone or tablet containing personal data that has been stolen remotely

Work out how many data subjects might be affected by the breach

We will find out how many people are affected by the breach. This will help determine the level of risk involved.

Assess the severity of the personal data breach

SHARE MAT will accurately record all details of the breach and make an assessment of the risk to the data subjects involved.

Risk, in terms of a personal data breach, means the risk to the people who are affected. The DPO will support to assess how seriously people might be harmed and the probability of this happening.

Consideration will be made of all the information currently available, for example:

- who's affected
- how many people are affected
- the ways it might affect them, such as:
- safeguarding issues
- identity theft
- significant distress

Report the personal data breach

If it is decided that there is a risk to data subjects:

- the DPO will notify the Information Commissioner's Office within 72 hours of becoming aware of it
- inform data subjects, so they can take steps to protect themselves.

Review the personal data breach

After every personal data breach or near miss, the DPO will review:

- what happened
- how it happened
- why it happened
- what actions you can take to prevent it happening again
- document all lessons and actions taken in order to reduce the possibility of personal data breaches occurring. This includes:
- having mandatory data protection training in place for all staff that includes how to recognise and report a personal data breach
- having clear and appropriate data protection policies
- ensuring staff have an awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails
- having appropriate controls in place to protect personal data.

13. Generative Artificial intelligence (AI) and data protection in schools

Generative AI refers to any type of artificial intelligence that creates new digital content, such as text, images, videos or other data. Unlike traditional AI, which relies on exact programming to complete specific tasks, generative AI uses machine learning to create new digital content.

In SHARE MAT, generative AI tools can be used as a starting point to develop resources, including:

- lesson plans or activities
- questions and quizzes
- revision activities
- images to help with character descriptions or stories
- communications for parents and carers
- creating timetables.

Please refer to the SHARE MAT Artificial Intelligence Policy & Procedure for further information.

Data Protection and AI tools in education

Generative AI tools can offer significant benefits in education, but they come with certain risks related to data protection. SHARE MAT are open and transparent about how they use generative AI tools and more detailed information can be found in the trust's Artificial Intelligence Policy & Procedure.

Open and closed generative AI

There are important differences between open and closed generative AI tools in terms of data protection.

Open generative AI tools are accessible and modifiable by anyone. They may store, share, or learn from the information entered into them, including personal or sensitive information. SHARE MAT avoid including any identifiable information in the data entered into open AI tools, to protect personal and special category data.

Closed generative AI tools are generally more secure, as external parties cannot access the data input. This makes them a safer option for handling personal or special category data.

It is not always obvious whether a generative AI tool is open or closed. Staff use open and closed generative AI tools in accordance with the SHARE MAT Artificial Intelligence Policy & Procedure and check with the Trust IT Manager for clarification if unsure.

Compliance with data protection legislation

The generative AI tools SHARE MAT use comply with data protection legislation and the trust's data protection notice.

In order to protect data when using generative AI tools, SHARE MAT staff:

- seek advice from the data protection officer or IT Manager
- check if it is an open or closed generative AI tool
- ensure there is no identifiable information included in open generative AI tools
- acknowledge or reference the use of generative AI when used
- fact-check results to make sure the information is accurate.

Personal data collected by generative AI tools

Some generative AI tools process and store more information than just the text you enter into them. Generative AI tools may collect and store additional data such as:

- location
- IP address
- system information
- browser information

The data collected by these organisations can be viewed or sold to third parties. The trust will include how any data is collected, processed and stored by generative AI tools in privacy notices.

14. Contact Us

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

Jayne Newson – Governance Professional and Data Protection Officer

Jayne.newson@sharemat.co.uk **Tel:** mailto: **08452 415175**

15. 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