Data Protection Policy

If you require this document in an alternative format please contact office@tssmat.staffs.sch.uk or 01543 472245

Last review date:	January 2026
Next Review date:	January 2027
Review Cycle:	Annually
Statutory Policy:	No
Owner	Business Manager
Publication:	Website. G/Policies

Date	Version	Reason for change	Overview of changes made	Source
10.12.20	0.1	Internal Lead Scheduled Review	Name & Logo update. Additional info on SAR charges. J Bowman	SCC
09.02.21	0.2	Board Lead Scheduled Review	No changes made. C Humphries.	
26.02.21	1.0	Board Scheduled Review	Policy ratified	
10.11.21	1.1	Internal Lead Scheduled Review	Incorporated FOI policy and publication scheme, Data Breach Policy, and GDPR monitoring policy Inclusion of Children's Code. Change from EEU to UK to reflect Brexit. J Bowman	
11.01.22	1.2	Board Lead Scheduled Review	Minor clarification to cost of SAR. C Humphries	
11.02.22	2.0	Board Scheduled Review	Ratified by Board	
29.11.22	2.1	Internal Lead Scheduled Review	Section 18 DPIA added. J Bowman	
17.01.23	2.2	Board Lead Scheduled Review	No changes. C Humphries	
27.01.23	3.0	Board Scheduled Review	Ratified.	
13.12.23	3.1	Internal Lead Scheduled Review	Addition of Appropriate Document.	
26.01.24	4.0	Board Scheduled Review	Ratified.	
14.01.2026	4.1	Board Lead Scheduled Review		

07.01.26	4.2	Internal Lead Scheduled Review	Updated to reflect Data (Use and Access) Act 2025. Refined SAR procedures to include "stop the clock" for clarifications and "proportionate" search standards. Added "Recognised Legitimate Interests" for safeguarding. Included new statutory 30-day acknowledgment period for data complaints. Updated regulator name to Information Commission (IC). J Bowman	Information Commissio n. DUAA 2025
06.02.26	5.0	Board Scheduled Review	Ratified.	

Data Protection Policy

Contents

1. Aims

The Staffordshire Schools Multi Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, Directors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018, and the UK Children's Code).

This policy applies to all personal data, regardless of format.

2. Legislation and guidance

This policy meets the requirements of the GDPR, the Children's Code and the DPA 2018. It is based on guidance published by the Information Commission (IC) the GDPR, the Data (Use & Access) Act 2025 and the IC's code of practice for subject access requests.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location 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 so needs more 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 ● Criminal record
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our Trust processes personal data relating to parents, pupils, staff, Directors, visitors and others, and therefore 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.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Trust, volunteers, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Directors

The Board of Directors has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 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.

The DPO will provide a summary of all data breaches to the Board of Directors at each meeting.

They will provide an annual report of their activities directly to the Board of Directors and, where relevant, report to the Board their advice and recommendations on Trust data protection issues.

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

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Jacqui Bowman and is contactable via dpo@tssmat.staffs.sch.uk or 01543 472 245

5.3 CEO

The CEO acts as the data controller on a day-to-day basis.

5.4 SLT

The SLT has oversight of data protection within their schools, and are responsible for ensuring the Data Protection Policy, Privacy Notices, and Record Retention Schedule are followed by staff within the school. They report to the CEO at the SLT meeting. Appropriate items are then included in the CEO's report to the Board.

5.5 School Data Protection Lead

The School's Headteacher is the Data Protection Lead for the school, as outlined in SLT above.

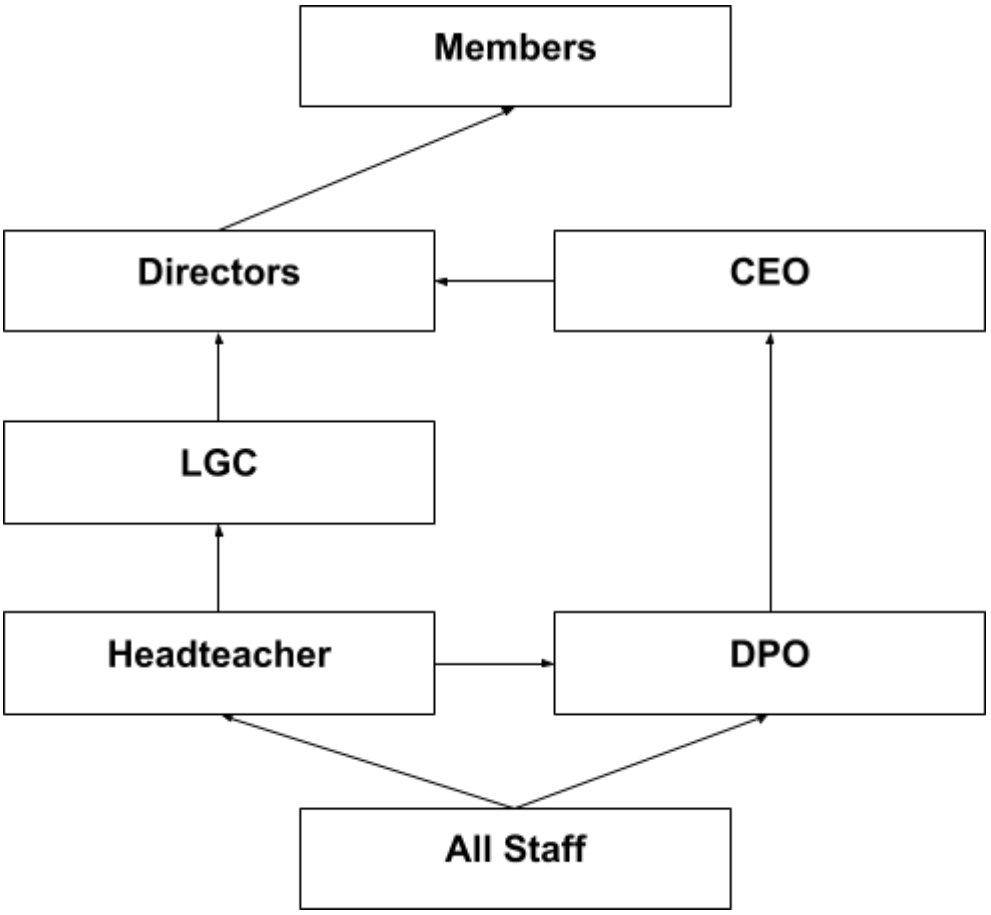
5.6 All staff

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, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a 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

5.7 Overview of Governance Structure



6. Data protection principles

The GDPR is based on data protection principles that our Trust must comply with.

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.

7. Collecting personal data

- Information will only be gathered and stored for specified purposes.
- In order to be able to respond to requests for information the Trust will implement effective records management policies to enable staff to identify whether data is held and, if it is, locate it quickly and easily.
- The Trust's retention policies will be based on the guidance in the Information and Records Management Society's Records Management toolkit for Trusts and will be reviewed regularly in line with any updates to this toolkit.
- Information held by the Trust will be regularly reviewed with a view to archiving or destruction, where appropriate.

7.1 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 Trust may process data without a separate "balancing test" (Legitimate Interest Assessment) where the processing is for a "recognised legitimate interest" defined by law. This includes:
    - **Safeguarding:** Sharing information to protect vulnerable individuals or children.
    - **Emergency Response:** Sharing data with emergency services or local authorities during a crisis.
    - **Crime Prevention:** Detecting and preventing crime or fraud.
- 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 (except for online counselling and preventive services).

7.2 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.

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.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule.

Staff and pupil contact and consent data is checked annually by the subject/subject's parents for accuracy. Any challenges to accuracy made through this process go to the school secretary, who rectifies the data on the school system immediately. These changes are not recorded.

Other challenges to accuracy can be made in writing to the school Head or DPO, who will look into the matter immediately, and rectify where necessary. These challenges and rectifications will be recorded on the Data Accuracy Register.

The Board reviews the Information Asset Register annually to ensure that data collected is for specified, explicit and legitimate purposes, is the least amount of data possible to fulfil the function, and is only kept for the minimum amount of time necessary.

8. Sharing personal data

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

- 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 seek consent as necessary before doing this
- We need to undertake audits as required by internal practice, or legislation
- 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
    - 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 for:

- 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 UK, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- 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

Subject access requests should be submitted in writing, either by letter or email to the DPO. They should include:

- 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 inform the DPO and forward the details of the request.

Applicants will be made aware that SAR's made within Trust holidays may be delayed.

9.2 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 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.

9.3 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
- Will respond without delay and within 1 month of receipt of the request
- Will conduct a search for the requested information that is "reasonable and proportionate". The Trust is not required to carry out exhaustive searches that would impose an undue burden.
- May ask for clarification before processing the request if it is broad or unclear. In such cases, the one month response period will be "paused" until the requester provides the necessary clarification. The clock will resume once clarification is received.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- 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.

A request may also be deemed to be excessive if it is likely to take more than one day of a staff member's time to collate all of the data. In this case, we may charge an hourly rate for the staff member's time for anything over one day's work, up to a maximum of one week's work.

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

9.4 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 UK

- 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.

Formal Complaints Process Under the Data (Use and Access) Act 2025, individuals have a formal right to complain to the Trust regarding the handling of their personal data.

- **Submission:** Complaints should be sent in writing to the DPO at [Insert Email].
- **Acknowledgment:** The Trust will acknowledge receipt of a data protection complaint within **30 days**.
- **Resolution:** We will investigate and provide an update on the outcome or progress of the complaint without undue delay. If the complainant remains dissatisfied, they retain the right to escalate the matter to the Information Commission.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, may access their child's educational record (which includes most information about a pupil) within 30 school days of receipt of a written request.

11. Photographs and videos

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

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.

Uses may include:

- Within Trust on notice boards and in Trust magazines, brochures, prospectuses, newsletters, etc.
- Outside of Trust by external agencies such as the Trust photographer, newspapers, campaigns
- Online on our Trust website or social media pages

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. Any printed material will be amended for the next print run. Uploaded material will be taken down as soon as reasonably possible.

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.

See our Photographs & Images Policy for more information on our use of photographs and videos.

12. 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 data protection impact assessments where the Trust's processing of personal data presents a 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

13. 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:

- 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, or printed at home, staff must ensure their Headteacher is aware that this is the case. Any paper based documents containing personal or confidential data taken off Trust premises are the responsibility of the member of staff/Director removing or printing. All documents must be kept securely, and securely destroyed as soon as they are no longer needed, or returned to Trust premises for appropriate storage and retention.
- Passwords that are at least 8 characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Staff 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
- USB devices should not be used without prior permission from the Headteacher
- Pupil iPads are expected to have their memory wiped after use
- Pupil iPads will have their memory wiped at least termly by the IT Technician
- Where cameras are used, no images will be stored on the camera's hard drive. All images must be stored on a memory card, which is kept securely, and wiped as soon as images have been uploaded to the secure network
- Staff, pupils or Directors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment. (See our Acceptable Use of IT 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 (see section 8)

The Trust will refer to its Cyber Security document, associated Action Plan and Risk Assessment, in order to protect its electronic data.

14. Record Retention

Data will be held in accordance with our Record Retention Schedule.

15. Disposal of records

The Trust will carry out data cleansing every July. Personal data that is no longer needed (in line with our retention schedule) 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 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.

16. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

16.1 Definition of a Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. TSSMAT understands that a personal data breach isn't only about loss or theft of personal data. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

Personal data breaches can include, but are not limited to:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

16.2 Recognising a Data Breach

All staff will receive annual training on recognising data breaches, in addition to input at Induction.

All staff **<u>are required</u>** to report a data breach if witnessed or found immediately to the DPO and their relevant Headteacher, using the TSSMAT Data Breach Register. The DPO or Headteacher will inform the Chief Executive Officer, who will inform the relevant Director(s).

It is the notifying member of staff's responsibility to ensure the DPO and/or Headteacher are aware of the data breach, if they are not available, staff must contact another Headteacher and/or the Chief Executive Officer to ensure that a relevant person is aware of the breach, and has taken responsibility for co-ordinating action.

If action can be taken by staff immediately to correct or halt the data breach, this should be done. All actions should be noted on the TSSMAT Data Breach Register by the DPO as soon as reasonably possible.

16.3 Personal data breach procedure

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. Staff, volunteers or other parties working for the Trust are required to fully engage in any data breach investigation. Failure to do so may be a disciplinary matter.
- The DPO will alert the Headteacher, and CEO. The Chair of Directors may also be notified.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress).
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's M Drive.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours.
- If all the details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. Records of all breaches will be stored on M/Data Protection
- The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

16.4 DPO Response to a Data Breach

The Data Protection Officer (DPO) for TSSMAT is the Trust Business Manager.

The DPO will be notified of all data breaches, internally and externally, via the TSSMAT Data Breach Report Form. The DPO's role is to co-ordinate the response to the breach, ensure corrective action is taken, and relevant bodies/individuals are notified if appropriate. If the DPO is not available, this role will fall to the Headteacher of the school the breach is relevant to, or the Chief Executive Officer if the breach concerns the MAT.

On receipt of the TSSMAT Data Breach Report Form, the DPO will ensure the relevant Headteacher, and the Chief Executive Officer are aware of the breach. The Chief Executive Officer will ensure the relevant Director(s) are aware of the breach.

The DPO will carry out an investigation into the breach using the Data Breach Investigation Report Form. The DPO will document the facts relating to the breach, its effects and the remedial action taken when and by whom.

The DPO will be responsible for informing the ICO or other relevant data protection agency (See Notifying the ICO), and affected individuals. The DPO is responsible for keeping the ICO/other DPA up to date as more information is gathered.

A report on data breaches will be presented to the Board of Directors at each meeting.

Records of data breaches will be kept in line with reports to the Board of Directors for 7 years.

16.5 Notifying the ICO or relevant International data protection agency about a Data Breach

If the ICO or other relevant data protection agency require notification, this will be done within 72 hours of TSSMAT becoming aware of the breach, even if full information is not available. To notify the ICO of a personal data breach, the DPO will use the ICO pages on reporting a breach.

TSSMAT will ensure the following information is provided, as soon as known, when notifying of a breach:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

16.6 Notifying affected individuals of a Data Breach

If a breach has occurred, TSSMAT will inform those concerned directly and without undue delay, if the breach has or may result in severe risk to individuals or companies.

TSSMAT will ensure the following information is provided, as soon as known, when notifying affected individuals of a breach:

- the name and contact details of the TSSMAT data protection officer, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.
- As with any security incident, you should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

This procedure is based on guidance on personal data breaches produced by the ICO.

Please see the Data Breach Procedure for more information

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed
- Made available where it should not have been
- Made available to unauthorised people

- The DPO will alert the Headteacher, and CEO. The Chair of Directors may also be notified.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

(Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's M Drive.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on G/Data Protection

The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

16.7 Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Personal data being disclosed via email (including safeguarding records)

- *If personal or special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*

- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will make a decision as to whether the ICO or the data subjects need to be notified, and carry this out where necessary*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *The DPO will conduct an investigation, and ensure lessons learnt are fed back to staff*

Personal data being disclosed via post

- *If personal or special category data is accidentally made available via post to unauthorised individuals, the sender must inform the DPO as soon as the error is realized*
- *The DPO will make a decision as to whether the ICO or the data subjects need to be notified, and carry this out where necessary*
- *the DPO will contact the relevant unauthorised individuals who received the post, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *The DPO will conduct an investigation, and ensure lessons learnt are fed back to staff*

Personal data being uploaded to the website

- *The data must be removed as soon as the error is realised, and the DPO notified.*
- *The DPO will make a decision as to whether the ICO or the data subjects need to be notified, and carry this out where necessary*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *The DPO will conduct an investigation, and ensure lessons learnt are fed back to staff*

Personal data being left unattended

- *The data must be stored securely as soon as the error is realised, and the DPO notified.*
- *The DPO will make a decision as to whether the ICO or the data subjects need to be notified, and carry this out where necessary*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *The DPO will conduct an investigation, and ensure lessons learnt are fed back to staff*

16.8 Media Plan

If necessary, a media plan will be developed by the CEO and Chair of Directors. This will include nominated members of staff who are able to speak to the Media, development of key messages, and a timetable for updated information to be released.

17. Freedom of information

The Freedom of Information Act 2000 (FOIA) was introduced to promote greater openness and accountability across the public sector and requires all maintained schools and Academies to be clear and proactive about the information they will make public.
As a result, we at The Staffordshire Schools Multi Academy Trust have produced a publication scheme, as recommended by the DfE, Information Commissioner and Staffordshire County Council, and approved by Trust Directors ,setting out:

- The classes of information which we publish or intend to publish;
- The manner in which the information will be published; and
- Whether the information is available free of charge or on payment.

The scheme covers information already published and information which is to be published in the future. All information in our publication scheme is available in paper form, some is available electronically on our website for you to download and print.

Some information which we hold may not be made public, for example, personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner's Office (ICO).

The Trust will comply with:

- The terms of the Freedom of Information Act 2000 and any other relevant legislation to ensure requests for access to information held by the Trust are treated in a manner that is fair and lawful.
- Staffordshire County Council advice and guidance.
- Information and guidance displayed on the Information Commissioner's website: https://ico.org.uk/

17.1 How to Request Information

If you require a paper version of any of the documents within the scheme, the request must be made in writing by email or letter giving clear details of the information requested.

Written notice of any fee will be provided to the enquirer before any information is supplied.
Contact details are set out below:
Address: The Staffordshire Schools Multi Academy Trust, Crawley Lane, Kings Bromley, Burton on Trent, DE13 7JE
Telephone: 01543 472 245
E-mail: dpo@tssmat.staffs.sch.uk
Web: www.tssmat.staffs.sch.uk

To help us process your request quickly, please clearly mark any correspondence “PUBLICATION SCHEME REQUEST” (in CAPITALS please).

If the information you’re looking for isn’t available via the scheme and isn’t on our website, you can still contact the school to ask if we have it.

17.2 Dealing with Requests for Information

Theoretically any request for information is a request under the Freedom of Information Act, however this Trust has taken the decision that it will not consider any request that forms part of the normal pattern of work to be a Freedom of Information request. Only those requests which are considered to be outside the normal remit of the service provided will be recorded as Freedom of Information requests.

The Trust will assist applicants in making their request to have access to information held by the Trust. Assistance will be given to applicants whose requests need to be transferred to another public authority (e.g. Trust, council, hospital).

The Trust will exercise its duty to confirm or deny the existence of requested data, subject to any exemptions that may apply.

The Trust will supply data requested within 20 working days (or in line with the Information Commissioner’s current policy during Trust holidays), subject to any exemptions that may apply, and the estimated cost of complying with the request falling within the current defined charge limit. All requests for information will still be dealt with in compliance with the 20 working day deadline, whether they are recorded as Freedom of Information requests or not.

If a response will take longer than 10 working days to respond an acknowledgement will be sent to the person making the request, informing them when the information will be supplied. We recognise this does allow the Trust to exceed the overall 20 working day deadline.
The charge limit is currently £450, calculated at 18 hours work at a flat rate of £25 per hour, as set by government statute. If the estimated cost of complying with the request does not exceed this amount the Trust is not entitled to make a charge for fulfilling the request.

Information published on our website is free, although you may incur costs from your Internet service provider. If you don’t have Internet access, you can access our website using a local library or an Internet café.

Single copies of information covered by this publication are provided free unless stated otherwise in section 6. If your request means that we have to do a lot of photocopying or printing, or pay a large postage charge, or is for a priced item such as some printed publications or DVDs we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated by a £ sign in the description box.

A designated member of staff will be responsible for ensuring requests are fulfilled within the stipulated deadline and recording details of the request on the Trust’s tracking database.

Persons requesting data will be supplied with a copy of our complaints procedure upon request.

Any complaints regarding Freedom of Information requests must firstly be addressed by the Trust. If, once we have had opportunity to reconsider our decision, we believe the initial response was correct the applicant shall be entitled to take the matter to the Information Commissioner's Office and, ultimately, to an Information Tribunal.

Copies of data supplied will be retained for two years from the date it was put into the public domain.

17.3 Applying Exemptions

A full list of exemptions can be found at the Information Commissioner's website. There are two types of exemption – absolute and qualified. In practice there are very few which are likely to be applied by the education sector.

The decision to apply absolute exemptions will not be taken by individual members of staff but by a constituted group of at least three of the following: Chair of Directors, other Directors, CEO, Headteacher.
The decision to apply qualified exemptions will not be taken by individual members of staff but by a constituted group of at least three of the following: Chair of Directors, other Directors, CEO, Headteacher. Even if the group decides information should not be disclosed, a public interest test will be carried out when applying qualified exemptions, to decide whether the public interest in disclosure outweighs the objection to disclosure. If it does the information must be disclosed.

Advice will be sought from Staffordshire County Council's Information Governance Team or Legal Services if there is any doubt as to whether information should be disclosed.

17.4 Logging Requests Received

The Trust will keep a record of all requests received for monitoring purposes (Appendix 1), noting:
a) the date the request was received,
b) name and contact details of the person or organisation making the request,
c) the date the request was fulfilled or refused,
d) the reason for any exemption being applied,
e) the reason for any failure to meet the 20 day deadline.

18. Data Protection Impact Assessments

Data Protection Impact Assessments (DPIA) are a process to help identify and minimise the data protection risks of a project. The Trust will undertake a DPIA for processing that is **likely to result in a high risk** to individuals, and for any other major project which requires the processing of personal data.

Our DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals;
- identify any additional measures to mitigate those risks

To assess the level of risk, the Trust will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The Data Protection Officer will complete the DPIA with input from relevant staff and stakeholders. If the Trust identifies a high risk that it cannot mitigate, the Trust will consult the ICO before starting the processing.

19. Training

All staff and Directors are provided with data protection training as part of their induction process.

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

20. Monitoring arrangements

Compliance with GDPR and other data protection legislation will be carried out on a rolling programme, as outlined annually in the Compliance Schedule. The Compliance Schedule includes auditing of relevant files, data protection walks, and data quality checks.

This procedure applies to all areas of the organisation where personal data and/or special category data is processed. This includes the processing operations carried out by Board members, the Senior Leadership Team, and all employees and workers.

20.1 Accountabilities and Responsibilities for Monitoring

The data controller is ultimately accountable for ensuring compliance with the GDPR. The data controller is responsible for ensuring that appropriate and proportionate technical and organisation measures are implemented to achieve compliance. The Senior Leadership Team will undertake a review of the measures for data protection (including cyber security) on an annual basis.

The Data Protection Officer (DPO) will be responsible for facilitating compliance with the GDPR, undertaking monitoring activity to an agreed plan and reporting the findings to the Senior Leadership Team.

All employees and workers are responsible for cooperating with the DPO during monitoring visits and engaging in the process.

The manager responsible for the area of the organisation being monitored is responsible for ensuring that the findings and agreed recommendations from the monitoring visit are implemented and that agreed corrective or preventive action is taken within the specified timescale.

20.2 Programme of Monitoring Visits

Monitoring visits will be carried out in accordance with the organisation's GDPR Annual Monitoring Plan. The plan is determined by the Senior Leadership Team in discussion with the DPO at the end of each academic year in readiness for the next year. Visits are planned throughout the year assessing and reviewing all the organisation's technical and organisational measures over

time.

The visits are led by the DPO. The DPO will arrange the date of the monitoring visit with the manager of the area to be monitored. The DPO will remind the manager of the audit 1 week prior to the visit. A monitoring visit should be given priority so it occurs on the planned date.

20.3 Conducting Monitoring Visits

- At the start of the monitoring visit, the DPO will meet with the manager (or nominated representative) to explain the scope of the visit and the process that is to be followed.
- The DPO will check any corrective action from the previous monitoring visit.
- The DPO will conduct the monitoring visit (see Appendix 3 – Guidance for Conducting Monitoring Visits) reviewing and recording evidence against the areas for monitoring. The detail of this will be recorded on the GDPR Monitoring Report form.
- At the end of the monitoring visit, the DPO will conduct a closing meeting with the manager (or nominated representative). At this meeting, a brief overview will be given of the findings and any immediate concerns are discussed and action agreed. The manager is responsible for taking action for each non-conformance or observation found.
- The DPO forwards the completed GDPR Monitoring Report to the Headteacher within 10 working days. The Headteacher is responsible for ensuring that any corrective action is taken within the agreed timeframes.
- The Headteacher will agree a date within the term for the DPO to conduct a follow up visit to check that the agreed corrective action has been implemented.

20.4 Monitoring Visit Outcomes

A three-tier system is used to record conformance/non-conformances as follows:

Conformance – policies, procedures, processes and working practices are in place and are delivering data protection compliance.

Non-conformance – policies and/or procedures and/or processes and/or working practices are identified as a significant risk and data protection compliance will not be achieved. Action is required to ensure compliance.

Observation – policies and/or procedures and/or processes and/or working practices need to be improved to reduce the risk of non-compliance with data protection requirements. Action is required to reduce the risk.

Corrective action is activity which corrects the immediate non-conformance, establishes the cause and takes steps to prevent a recurrence. When a non-conformance is identified in the course of a monitoring visit, the DPO will plan a follow up visit, one month after the event, to verify that the

non-conformance has been corrected.

Preventive action aims to prevent the occurrence of problems, deviation and breaches. If during a monitoring visit, a policy, procedure or working practice is found to be either out of date, inaccurate or in need to review to reflect the requirements of the GDPR, this will be recorded by the DPO. The manager for that area will be responsible for reviewing the policy, procedure or working practice.

20.5 Review of Monitoring Process

On an annual basis, the Senior Leadership Team will review this monitoring process and the outcomes from monitoring visits (see Appendix 4 – Management Review), before setting the GDPR Annual Monitoring Plan for the next year. The outcomes of the management review should be reported by the CEO to Board of Directors to further demonstrate accountability and compliance with the GDPR.

21. Links with other policies

This data protection policy is linked to our:

- E- Safety Policy
- Acceptable Use of IT Policy
- Safeguarding Policy
- Use of Photographs and Images Policy

Appendix 1.

Freedom of Information Request Log

APPENDIX 1 – TSSMAT LOG OF FOI REQUESTS RECEIVED

Date the request was received		Name & contact details of the person or organisation making the request	Date the request was fulfilled or refused	Reason for any exemption being applied	Reason for any failure to meet the 20 day deadline
Date	Name of staff recording request				

Appendix 2.
Freedom Of Information Publication Scheme

The Board of Directors is responsible for maintenance of this scheme.

Categories of information published
The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'. These are contained in section 6 of this scheme.

The classes of information that we undertake to make available are organised into four broad topic areas:

School Prospectus – information published in the school prospectus (non-statutory from Sept 2012)
Directors' Documents – information published on the school website and in other Board documents.
Pupils & Curriculum – information about policies that relate to pupils and the school curriculum.
School Policies and other information related to the Trust/school - information about policies that relate to the Trust or school in general.

Classes of Information Currently Published

Director's Documents and other information relating to the governing body– this section sets out information published on the school website and in other governing body documents.

Class	**Description**
Pupil Premium	• The allocation of funding to the school, its use and impact on attainment.
Sport Premium	• The allocation of funding to the school, and its use
Instrument of Government	• The name of the school • The category of the school • The name of the governing body • The manner in which the governing body is constituted • The term of office of each category of Director if less than 4 years • The name of any body entitled to appoint any category of Director • Details of any trust • If the school has a religious character, a description of the ethos • The date the instrument takes effect
Minutes of meeting of the governing body and its committees	Agreed minutes of meetings of the governing body and its committees *[current and last full academic school year]*

Curriculum, School Policies and other information related to the school - This section gives access to information about policies that relate to the school in general.

Class	Description
Published reports of Ofsted referring expressly to the school	Published report of the last inspection of the school and the summary of the report and where appropriate inspection reports of religious education in those schools designated as having a religious character
Post-Ofsted inspection action plan	A plan setting out the actions required following the last Ofsted inspection and where appropriate an action plan following inspection of religious education where the school is designated as having a religious character
Charging and Remissions Policies	A statement of the school's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted, for example school publications, music tuition, trips
School session times and term dates	Details of school session and dates of school terms and holidays
Health and Safety Policy and risk assessment	Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy
Complaints policy & procedure	Statement of procedures for dealing with complaints
Performance Management of Staff	Statement of procedures adopted by the governing body relating to the performance management of staff.
Staff Conduct, Discipline and Grievance	Statement of procedure for regulating conduct and discipline of school staff and procedures by which staff may seek redress for grievance
Policy Statements	Policies are available on the Trust website. If you cannot find the policy you are looking for, please contact the Trust

Feedback and Complaints

We welcome any comments or suggestions you may have about the scheme. If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint then initially this should be addressed to the Chair of the Board of Directors.

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Freedom of Information Act 2000 and that deals with formal complaints. They can be contacted at:

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Enquiry/Information Line: 01625 545 00
E Mail: publications@icfoi.demon.co.uk

Website: www.informationcommissioner.gov.uk

Appendix 3 – Guidance for Conducting Monitoring Visits

1. Carry out the monitoring visit in accordance with the GDPR Annual Monitoring Plan and organisation's policy.

2. Check the status of previous non-conformances or observations raised; these should have been addressed and any corrective or preventative actions implemented and monitored by the manager following the previous visit.

3. Confirm with the manager that this has happened. If not, obtain a copy of the previous monitoring report and check that corrective action has been taken in all instances.

4. Note any specific instances of non-conformity with documented procedures and/or with the General Data Protection Regulation pertaining to the area.

The monitoring report should include:

- The scope of the visit (areas or functions to be checked and how);
- Specific non-conformances or observations;
- Suggested corrective action, where appropriate; and
- Instances where existing documented procedures are not fully effective to meet the General Data Protection Regulation requirements

5. The monitoring report should be given as soon as completed to the manager and Headteacher.

6. Where non-conformity is detected with existing documented procedures, the document owner will be notified by the DPO and requested to conduct a review of the procedure within a month. Other stake holders involved in the process subject to review must be invited to assist in the review.

7. The monitoring report must be completed in full and a copy retained securely by the DPO.

Appendix 4 – Management Review

When reviewing the monitoring process, the Senior Leadership Team should consider the following areas:

Area for Review	Detail	Responsibility
Follow Up	Follow up of actions from previous management review.	All
Data Protection Policy	Review of the suitability and implementation of data protection policy/policies.	All
GDPR	Review of data and logs to confirm that technical and organisational measures are sufficient in ensuring compliance with the GDPR and to identify any improvements that be made or preventive action that can be taken.	DPO
Process Performance	Review of the monitoring process to ensure it performs satisfactorily and the outputs are effective in ensuring compliance.	All
Internal Monitoring	Review of the monitoring visit carried out. SLT to decide whether any significant changes need to be made to the monitoring system as a result of the findings.	DPO
Improvements and Preventive Action	Are there any other measures that could be taken to improve compliance with the GDPR? Have any appropriate preventive actions been identified?	All
Process Changes	Planned changes to the organisation's operations. Discussion on whether they could impact on the effectiveness of the existing monitoring system.	All
External Audits	Review of any audits related to GDPR carried out by external agencies. Do the findings/outcomes	DPO

	broadly agree with the internal monitoring process? Is any action required?	
Any other Matters	For example, any changes in legislation or significant organisational change which may impact on compliance	All