Severn Bridges Multi-Academy Trust

Data Protection Policy

Approval Date:	July 2025
Approved By:	Severn Bridges Multi-Academy Trust Board
Policy Review Date:	July 2026

Severn Bridges Multi-Academy Trust | Greenfields Primary School | Mount Pleasant Primary School & Nursery | Radbrook Primary School | Sundorne Infant School & Nursery | Harlescott Junior School

Aims

Our Severn Bridges Multi-Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and Guidance

This policy meets the requirements of the UK GDPR* and the DPA 2018**

**The EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020.*
***Data Protection Act 2018 (DPA 2018)*

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence (AI) in education.

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

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 is more sensitive 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

Processing	Any 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.

The Data Controller

Severn Bridges Multi-Academy Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. Severn Bridges Multi Academy Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

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

Governing Board

The Trust Board has overall responsibility for ensuring that Severn Bridges Multi Academy Trust complies with all relevant data protection obligations

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Severn Bridges Multi-Academy Trust data protection issues.
The DPO is also the first point of contact for individuals whose data Severn Bridges Multi Academy Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.
Our DPO is:
SchoolPro TLC

T: 01452 947 633
E: dpo@schoolpro.uk

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

All Staff

Staff are responsible for collecting, storing and processing any personal data in accordance with this policy.

Informing Severn Bridges Multi Academy Trust of any changes to their personal data, such as a change of address or 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.

Data Protection Principles

The UK GDPR is based on data protection principles that Severn Bridges Multi-Academy 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 school aims to comply with these principles.

Collecting Personal Data

Lawfulness, Fairness and Transparency

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

1. The data needs to be processed so that Severn Bridges Multi Academy Trust can **fulfil a contract** with the individual, or the individual has asked Severn Bridges Multi Academy Trust to take specific steps before entering into a contract.
2. The data needs to be processed so that Severn Bridges Multi Academy Trust can **comply with a legal obligation**.
3. The data needs to be processed to ensure the **vital interes**ts of the individual e.g. to protect someone's life.
4. The data needs to be processed so that Severn Bridges Multi Academy Trust, as a public authority, can **perform a task in the public interest**, and carry out its official functions.
5. The data needs to be processed for the **legitimate interests** of Severn Bridges Multi Academy Trust or a third party (provided the individual's rights and freedoms are not overridden).
6. 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 UK 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).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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. We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be erased when appropriate. 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 Severn Bridges Multi Academy Trust record retention schedule.

Special Category Data

Severn Bridges Multi Academy Trust process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

Processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data. The information supplements our privacy notices.

We process special categories of personal data under the following UK GDPR Articles:

i. Article 9(2) (a) explicit consent, where we seek consent, we ensure the consent is unambiguous and for one or more specific purpose, an affirmative action is recorded as the condition for processing.
ii. Article 9(2) (b) performing or exercising obligations or rights that are imposed or conferred by law on the school or the data subject in connection with employment, social security or social protection.
iii. Article 9(2) (c) to protect the vital interests of the data subject or of another natural person.
iv. Article 9(2) (f) – for the establishment, exercise or defence of legal claims.
v. Article 9(2)(g) - reasons of substantial public interest.
vi. Article 9(2)(j) – for archiving purposes in the public interest.

Processing which requires an Appropriate Policy Document for the School

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

The processing of special category ('SC') and criminal offence ('CO') data based on the specific Schedule 1 conditions that is compliant with the requirements of the UK GDPR Article 5 principles. Our retention with respect to this data is documented in our retention schedules.

Special category data - Part 1 of Schedule 1

- Paragraph 1(1) employment, social security and social protection.

Special category data - Part 2 of Schedule 1

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) safeguarding of children and of individuals at risk

Criminal offence data - Parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2) (a) – statutory, etc. purposes
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc.
- Paragraph 18(1) – safeguarding of children and of individuals at risk
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest

Description of Data Processed

The special category data about our employees is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in our staff privacy notice.
We process the special category data about the children in our care and other members of our community that is necessary to fulfil our obligations as a school, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in our pupil privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

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
- 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 UK 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.

When doing this, we will:

- Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor 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

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 UK data protection law.

Subject Access Requests and Other Rights of Individuals

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Severn Bridges Multi Academy 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or
- to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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.
- The safeguards provided if the data is being transferred internationally.

Subject access requests must be submitted in writing, either by letter, email or fax 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 forward it to the DPO.

Children and Subject Access Requests

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at Severn Bridges Multi Academy 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.

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 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 being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- 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.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO https://ico.org.uk/

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 headed **Collecting Personal Data**), 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
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests

- Challenge 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

Parental Requests to see the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Biometric Recognition Systems

The school does not collect or otherwise process biometric data.

CCTV

In a few of our schools we use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's guidance for the use of surveillance systems including CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

Photographs and Videos

As part of our Severn Bridges Multi Academy Trust activities, we may take photographs and record images of individuals within our academies.

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 the school on notice boards, displayed in corridors and in Severn Bridges Multi Academy Trust prospectuses, newsletters, etc.
- Outside of school by external agencies such as newspapers, campaigns
- Online on our school/trust websites 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.

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.

Artificial Intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Severn Bridges Multi Academy Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

Only AI systems that meet UK GDPR standards and have been assessed for data minimisation, security, transparency, and retention practices will be used in school operations.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, Severn Bridges Multi Academy Trust will treat this as a data breach and will follow the personal data breach procedure outlined in **Appendix 1**.

Use of Generative Artificial Intelligence (AI)

Not to be confused with Artificial general intelligence, Severn Bridges Multi Academy Trust understands that generative AI is a valuable tool that serves many purposes. However, most crucially, the Trust also acknowledges the inherent dangers associated with these technologies, particularly concerning "sensitive and personal data". Due to these significant data concerns, Severn Bridges Multi Academy Trust currently maintains a policy of not using generative AI within its operations.

Cloud Computing

Cloud computing refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive.

This involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

When assessing any cloud-based or AI-powered service, the school will ensure that the provider demonstrates UK GDPR compliance, provides explicit guarantees regarding non-retention of input data, and allow the school to audit or verify compliance where necessary.

A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud.

A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. As with files on school devices, only authorised parties will be able to access files on the cloud.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the Headteacher.

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 9

- 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 headed Data Protection Principles)
- Completing privacy impact assessments where the school'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 school 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.

Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We will do a DPIA for processing that is likely to result in a high risk to individuals as well as any other major project that requires the processing of personal data.

It is vital that the DPIA is completed before processing is commenced to ensure that all risks are identified and mitigated as much as possible.

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; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, we 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.

We will consult our data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing. We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

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, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 Sharing Personal Data).

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

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

Personal Data Breaches

Severn Bridges Multi Academy Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours of becoming aware of it. Such breaches in Severn Bridges Multi Academy Trust context may include, but are not limited to:

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

DBS Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Training

All staff and governors 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 Severn Bridges Multi Academy Trust processes make it necessary.

Links with Other Policies

This Data Protection Policy is linked to our:

- Safeguarding Policy
- Freedom of Information Policy
- Online Safety Policy
- Network Security Policy

Monitoring and Review

This policy is reviewed at least annually and will be updated as needed to ensure it is up-to-date with such issues as they emerge and evolve, including any lessons learnt.

Any changes made to this policy will be communicated to all members of staff. All members of staff are required to familiarise themselves with all processes and procedures outlined in this policy as part of their induction programme.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO. 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 or made available where it should not have been
- Made available to unauthorised people.

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
The DPO will alert the headteacher and the chair of governors if a breach has occurred or if it is considered to be likely that is the case.
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, and the DPO should take external advice where necessary, e.g. from IT providers. (See the actions relevant to specific data types 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 before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool. 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 MAT's central team computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through its breach report line (0303 12311313) within 72 hours of the school's awareness of the data breach. 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 of the school's awareness of the data breach. 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:

- A description, in clear and plain language, of the nature of the personal data breach.
- 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 the MAT's central team computer system.

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

Actions to Minimise the Impact of Data Breaches

We will take action 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. An example of how we might mitigate a breach is outlined below we would take the same type of approach following any other data breach.

e.g. mitigation if sensitive information had been disclosed via email (including safeguarding records)

- *If 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*
- *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*

- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).*
- *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 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.*