SARACENS
MULTI-ACADEMY
TRUST

DATA PROTECTION POLICY

Responsibility of *(see policy tracking sheet):*	CFOO
Approved by:	CFOO
Approved *(by above):*	October 2025
Next Review due by:	October 2026

Contents

1. Statement of Intent

Saracens Multi-Academy Trust ("the Trust") is required to keep and process certain information about its staff, volunteers, pupils, parents/carers and governors/trustees in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018.

The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Department for Education (DfE), other schools and educational bodies, and potentially children's services.

This policy applies to all trustees, governors, staff and volunteers working for the Trust and its schools, and to external organisations and individuals working on behalf of the Trust. Staff who do not comply with this policy may face disciplinary action. This policy ensures all staff are aware of their responsibilities and outlines how its schools comply with the core principles of the UK GDPR as outlined in Section 7.

Organisational methods for keeping data secure are imperative. Saracens Multi-Academy Trust (SMAT) believes that it is good practice to keep clear, practical policies, where necessary backed up by written procedures.

This policy complies with the requirements set out in the UK GDPR.

2. Equal Opportunities and Inclusion

It is the right of all staff, volunteers, pupils, parents/carers and other individuals who come into contact with the Trust's schools, regardless of their gender, ethnicity, religion or beliefs, physical disability, ability, linguistic, cultural or home background, to have their personal information collected, stored and processed in line with the requirements of the current legislation.

3. Aims of this Policy

SMAT uses personal information about current and former staff, volunteers, pupils, parents/carers, local authority (LA) personnel, visitors and applicants and other individuals who come into contact with its schools. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the schools comply with their statutory obligations.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 2018 and the UK GDPR. It will apply to information regardless of the way it is used, recorded, stored and whether it is held in paper files or electronically.

This policy is issued on behalf of the Trust and its schools, where there is a reference to the Trust in this Policy, it is referring to the organisation responsible for processing personal and special category data. Any reference in this policy to a school is also a reference, where applicable, to the Trust.

4. Scope of the Policy

The Trust recognises that the correct and lawful treatment of personal data will maintain confidence in the Trust's schools. Protecting the confidentiality and integrity of personal data is a critical responsibility that the Trust takes seriously at all times.

The Trust collects a large amount of personal data every year including: staff records, names and addresses of those requesting information, examination marks, references, payment collection as well as the many different types of research data used by the schools. In addition, the schools may be required by law to collect and use certain types of information to comply with statutory obligations of LAs government agencies (including the DfE) and other bodies. Personal data means any information relating to an identified or identifiable natural person ('data subject').

As Data Controller, the Trust must ensure that personal data collected and held about staff, pupils, parents/carers, governors/trustees, visitors and other individuals must be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the DPA 2018.

5. Definitions of Data Protection Terms

Information Commissioner's Office (ICO) Notification and Registration	The Trust is required to 'notify' the Information Commissioner of the processing of personal data. This information is included in a public register which is available on the Information Commissioner's website. As the Data Controller, the Trust will register annually (or as otherwise required) with the ICO, as required by legislation.
Privacy Notices	Every member of staff, trustee, governor, other volunteer, contractor, and partner of the Trust that holds its personal information, must comply with the law when managing that information. The Trust's schools also have a duty to issue a privacy notice to all pupils, parents/ carers, governors/ trustees/ volunteers and staff; these provide details of information collected and held, why it is held and the other parties to whom it may be passed on.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
Data Controller	Is the organisation which determines the purposes for which, and the manner in which, any personal data is processed. It is responsible for establishing practices and policies in line with the data protection law. SMAT is the Data Controller of all personal data and special categories used within the Trust for operational purposes.
Data Privacy Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major

	system or business change programs involving the processing of personal data.
Data processor	Includes any person or organisation (that is not a data user) which processes personal data on behalf of the Trust and its schools and on its instruction. Staff employed by the Data Controller are excluded from this definition, but it could include suppliers which handle personal data on behalf of the Trust and its schools.
Data Protection Officer (DPO):	Is the individual or organisation appointed by the Trust to be responsible for monitoring the Trust's compliance with data protection law.
Data subject	Means a living, identified or identifiable individual about whom the Trust holds personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.
Data users	Trust staff whose work involves processing personal data. Data users must protect the data they handle in accordance with this Data Protection Policy and any applicable data security procedures at all times.
Personal data	Means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes any expression of opinion about an individual and intentions towards an individual. It includes information about pupil behaviour and attendance, assessment and exam results, staff recruitment information, contracts and appraisals and staff and pupil references. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.
Personal data breach	Any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that the Trust or its third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.
Processing	Is any activity which is performed on personal data such as collection, recording, organisation, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special category personal data	Includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union

	membership, physical or mental health or condition, genetic/biometric data held for purposes of identification or data about sexual orientation or an individual's sex life. Data about and safeguarding matters, pupils in receipt of pupil premium, SEND, Children in Need and Looked after Children are also treated as special category data.

6. Roles and Responsibilities

This policy applies to all personal data the Trust processes regardless of the media on which that data is stored or whether it relates to past or present pupils, staff, or supplier contacts, website users or any other data subject.

Trust Board

The Trust Board has overall responsibility for ensuring compliance with relevant data protection obligations. It monitors the data protection performance of the schools and Trust Office, supports the DPO, checks that the Trust has good network security infrastructure to keep personal data protected and has a business continuity plan in place that includes cyber security. All policies and documents related to data protection are approved by the Trust Board.

Chief Executive Officer (CEO) and Chief Financial and Operating Officer (CFOO)

These senior leaders are responsible for:

- deciding how the schools use technology and maintain security
- deciding what data is shared and how
- setting Trust policies for the use of data and technology
- understanding what UK GDPR and the Data Protection Act covers and getting advice from the DPO, as appropriate
- assuring trustees that the school has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive training on data protection every 2 years.

Staff, those working on behalf of the Trust and volunteers (including trustees and governors)

This policy applies to all school staff, and to external organisations or individuals working on the Trust's behalf.

All staff and volunteers must complete compulsory data protection training and comply with it when processing personal data on behalf of the Trust.

All staff and volunteers are responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- ensuring that personal data held is accurate and up to date
- ensuring that personal data held is not misused, lost or unlawfully disclosed.

Data Protection Team

The Data Protection Team (DPT) is made up of a Data Protection Officer (DPO), the Deputy Data Protection Officer (DDPO) (who is the Trust's CFOO) and the Head of IT. The team is

responsible for overseeing the implementation of this policy, monitoring the Trust and schools' compliance with data protection law, and developing related policies and guidelines, where applicable.

Data Protection Officer
The DPO is responsible for overseeing the implementation of this policy, monitoring the Trust's compliance with data protection law, and developing related policies, privacy notices and guidelines where applicable. The DPO will conduct regular data audits, advise when data impact assessments are needed and make sure that all assets containing personal data are appropriately managed and stored. The DPO will (in conjunction with the DDPO) provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on Trust and school data protection issues. The DPO is also a point of contact for individuals, whose data the Trust processes, who wish to raise any complaint regarding a school's processing where they remain dissatisfied with the Trust's response.

The DDPO in conjunction with the DPO will provide an annual report directly to the Trust Board and, where relevant, will report any advice and recommendations on individual school data protection issues.

The DDPO is also the first point of contact for individuals whose data the schools process, and for the ICO.

The DDPO can be contacted at: gdpr@saracensmat.org

The DPO is David Powell who can be contacted at: dpo@sapphireskies.co.uk

All staff must contact the Deputy DPO (DDPO) in the following circumstances:
- Where they are unsure or have questions about the operation of this policy; the purposes for which data may be used; retaining personal data; disclosing personal data or keeping personal data secure
- If there has been a data breach or a suspected data breach
- Where they are unsure if they have a lawful basis for processing personal data or wish to process for a different purpose than the one that the data was obtained
- Where they propose to engage in any activity that affects the rights of privacy of any individual i.e. where there is a legal obligation to carry out a Data Protection Impact Assessment (DPIA)
- Where they are unsure about what security, or other measures they need to implement to protect personal data
- If they are engaging in an activity that may affect the privacy rights of individuals
- If they need any assistance dealing with any rights invoked by a data subject
- Where they are considering sharing personal data with third parties
- Where they are entering into contracts involving the processing of personal data by another organisation
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual
- If they need to transfer personal data outside the European Economic Area (EEA).

Where staff or volunteers have concerns that this policy is not being followed by others, they should report this immediately to the DDPO. Where they wish to raise this formally, they may do so under the Trust's Confidential Reporting (Whistleblowing) Code.

7. Personal Data Protection Principles

SMAT adheres to the principles relating to the processing of personal data set out in the UK GDPR which require personal data to be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

SMAT is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Data subjects are allowed to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests) see Section 11.

The Trust is committed to maintaining the data protection principles at all times. This means that the schools will:

- Inform data subjects, via privacy notices about the processing of their personal and special category data. Who is it collected by, how is it being used and who is it shared with
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access request
- Train all staff so that they are aware of their responsibilities and of the Trust's relevant policies and procedures.

8. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. The Trust may only collect, process and share personal data fairly and lawfully and for specified purposes. The UK GDPR restricts the Trust's actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that the Trust processes personal data fairly and without adversely affecting the data subject.

The UK GDPR allows processing for specific purposes, some of which are set out below:

a) The data subject has given his or her consent
b) The processing is necessary for the performance of a contract with the data subject
c) To meet the Trust's legal compliance obligations
d) To protect the data subject's vital interests
e) To allow schools, as public authorities, to perform a task in the public interest, and carry out their official functions – this is known as the public task
f) To pursue the Trust's legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

For special categories of personal data, the Trust will also meet one of the special category conditions for processing which are set out in the UK GDPR and DPA 2018.

If the Trust's schools offer online services to pupils, such as classroom apps, and it intends to rely on public task, legal obligation and/or consent as a basis for processing, the Trust will obtain parental consent as necessary (except for online counselling and preventive services).

The purposes for which the Trust processes personal data to perform public tasks, are set out in the privacy notices issued by the schools.

When the Trust collects personal data directly from data subjects, including for human resources or employment purposes, it provides the data subject with all the information required by the UK GDPR. This information includes the identity of the Data Controller and DPO, and how and why the data will be used, processed, disclosed, protected and retained through a privacy notice.

Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. The Trust will explain these reasons to the individuals when first collecting their data.

If the Trust wants to use personal data for reasons other than those given when first obtained it, it will inform the individuals concerned before it does 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 Data Retention Policy.

9. Sharing Personal Data

The Trust will not normally share personal data with anyone else without express consent, but may do so where:

- It is necessary for the performance of a public task
- There is an issue with a pupil or parent/carer that puts the safety of another individual at risk
- For safeguarding purposes.

The ICO has provided guidance regarding sharing information for safeguarding purposes: a 10-step guide to sharing information to safeguard children. It is not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child. The Designated Safeguarding Lead (DSL) will decide if personal data needs to be shared.

The Trust's suppliers or contractors need data to enable the Trust to provide services to staff and pupils – for example, IT companies. When doing this, the Trust will:

(i) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

(ii) Establish either in the contract or as a standalone agreement, a data processing agreement to ensure the fair and lawful processing of any personal data shared by the Trust

(iii) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust.

The Trust and its schools will share personal data with law enforcement and government bodies where it is legally required to do so, including for the following purposes:

- 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 the Trust's safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The Trust may also share personal data with emergency services and LAs to help them to respond to an emergency situation that affects any pupils or staff and for safeguarding purposes.

Where the Trust transfers personal data to a country or territory outside the EEA, it will do so in accordance with data protection law.

The Trust and its schools may enter into information-specific sharing agreements with other public bodies for the purposes outlined above.

10. Consent

Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The schools ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 13, the consent of parents/carers will be sought prior to the processing of special categories of their data, except for safeguarding to prevent harm and where the processing is related to preventative or counselling services offered directly to a child.

When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

11. Subject Access Requests and Other Rights of Individuals

The Trust's data subjects have rights when it comes to how the Trust handles their personal data. These include rights to:

- withdraw consent to processing at any time
- receive certain information about how the Trust process their data
- request access to their personal data that the Trust hold
- prevent use of their personal data for direct marketing purposes
- ask the Trust to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- restrict processing in specific circumstances
- challenge processing which has been justified on the basis of the Trust's legitimate interests or in the public interest
- request a copy of an agreement under which personal data is transferred outside of the EEA
- object to decisions based solely on automated processing, including profiling (known as automated decision making (ADM))
- prevent processing that is likely to cause damage or distress to the data subject or anyone else

- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and
- make a complaint to the ICO.

How to make a subject access request
Subject access requests should be addressed to: gdpr@saracensmat.org

The Trust normally has one month to respond to a request.

UK GDPR requests for personal data are free in most cases unless the request is manifestly unfounded or excessive, when a "reasonable fee" for the administrative costs of complying with the request may be charged.

A reasonable fee will be charged based on administrative costs if an individual requests further copies of their data following a request.

When responding to requests, the Trust may ask the individual to provide two forms of identification and contact the individual to confirm that they made a request.

Where the request is complex or numerous requests have been made, the Trust may inform the requester within 1 month that it will comply within three months of receipt of the request, explaining why the extension is necessary.

The Trust will not disclose information if by doing so 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
- commercially sensitive information
- it is exempt under GDPR law.

When the Trust refuses a request, the individual will be advised of the reason and that they have the right to complain to the ICO.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents/carers of senior school pupils may not be granted without the express permission of the pupil. This is not a firm rule and a pupil's ability to understand their rights will always be decided on a case-by-case basis.

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

12. CCTV

The Trust uses CCTV in various locations around the school sites to ensure they remain safe. The Trust will adhere to the ICO's code of practice for the use of CCTV

The Trust does not ask individuals for permission to use CCTV, but makes it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Covert surveillance will only be allowed in exceptional circumstances.

The system and data collected will only be available to appropriate members of the school and Trust staff. The school Principals authorise access to the system as required, and review all access on an annual basis. In exceptional circumstances the CEO and CFOO may gain access to the system via the master administrative credentials held by the Trust's Head of IT.CCTV recordings will only be provided to third parties, such as the police, for investigative or public protection purposes and there is a lawful reason to do so.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.

Any enquiries about the CCTV system should be directed to the DDPO at:
gdpr@saracensmat.org

13. Photographs and Videos

As part of the Trust's schools' activities, the Trust may take photographs and record images of individuals within its schools.

The Trust will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the school's/SMAT websites or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photograph or video and not distribute it further.

Unless specific permission is given by parents/carers, when using photographs and videos in this way, the Trust will not accompany them with any other personal information about the child, to ensure the child cannot be identified.

14. Record keeping

UK GDPR requires the Trust to keep full and accurate records of all data processing activities.

The Trust keeps and maintains accurate records of data processing. These records include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage

locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

15. Accountability, Data Protection by Design

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

- Appointing a suitably qualified DPO
- 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
- 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; and keeping a record of compliance
- Regularly conducting reviews and internal audits to test privacy measures and to ensure compliance.

16. Data Security and Storage of Records

Organisations including schools and colleges, are required to take security measures to mitigate the risks of unauthorised destruction of data, unauthorised disclosure of data, unauthorised access to data and any unauthorised alteration of it. The Trust will ensure staff are aware of risks and how to minimise them. The Trust will put measures in place to reduce the risk of Cyber Attacks (see the Trust's Data Security Policy). The Trust will comply with current DfE Cyber Security Standards in School and Colleges: Meeting digital and technology standards in schools and colleges.

SMAT has a responsibility to maintain its records and record keeping systems. When doing this, the Trust will take account of the following factors:

- The most efficient and effective way of storing records and information
- The confidential nature of the records and information stored
- The security of the record systems used
- Privacy and disclosure; and
- Their accessibility.

The Trust 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.

By way of example:

a. At the commencement of each academic year, staff will complete an ICT Acceptable Use Agreement confirming that where personal information needs to be taken off site, they will handle it securely in accordance with this policy
b. Passwords that comply with current best practice are used to access school computers, laptops and other electronic devices
c. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
d. Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see

the Trust's and Schools' ICT Acceptable Use Policy and Agreements)

e. Where the Trust needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see Section 9)

17. Filtering and Monitoring

As part of its safeguarding responsibilities, the Trust has a duty to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn. As part of this duty, governors/trustees should limit pupils' exposure to risks from the schools' IT system, ensure that schools have appropriate filtering and monitoring systems in place, and regularly review their effectiveness in accordance with published DfE Guidance on Filtering and Monitoring.

All staff should have an awareness and understanding of the provisions in place, manage them effectively and know how to escalate identified concerns.

18. 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 the Trust cannot or do not need to rectify or update it.

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

The Freedom of Information Act 2000 requires the Trust to maintain a list of records that have been destroyed and who authorised the destruction. A record will be kept of who authorised the destruction and a brief description of the data and number of files destroyed.

19. Personal Data Breaches

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

In the unlikely event of a suspected data breach, the Trust will follow the procedure set out in Appendix 1.

When appropriate, the Trust will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

a. A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
b. Safeguarding information being made available to an unauthorised person.

20.Cyber Awareness Plan – Training and Acceptable Use

All staff and governors/trustees 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 school's processes make it necessary.

Train students and staff

Training students and staff in cyber security is a vital step in maintaining safety and security. Cyber training should be given at least annually, or more regularly if there is a known cyber risk to those who use school or college digital technology.

The SLT digital lead will need to coordinate training with IT, the DPO and the designated safeguarding lead. This training is for:

- students
- staff
- at least one current governor or trustee
- anyone else with a login (for example supply teachers or agency workers) who may need more focussed training using your own resources – this should happen as soon as it's feasible

Training should be age-appropriate and suited to your school or college's risks, but should generally include training on:

- methods hackers use for tricking people into disclosing personal information, including phishing
- password security
- online safety
- social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- the physical security of devices, for example not leaving a laptop unlocked and unattended
- the risks of using removable storage media, such as USBs
- multi-factor authentication
- how to report a cyber incident or attack
- how to report a personal data breach
- data protection for all staff, with staff who are exposed to higher risk data having more frequent training, such as administrative staff, management or agency workers with a login

Create an acceptable use policy

- An acceptable use policy describes what a person on the network can or cannot do when using digital technology.
- Anyone who has access to the school or college network or data will need to be made aware of, and sign up to, the acceptable use policy. This will include guests and supply teachers who want to use the school or college network and wifi.
- **The SLT digital lead and or other appropriate member of staff will work with IT, the designated safeguarding lead and the DPO where possible to create and update the acceptable use policy.**

21. Cyber Risk Assessment

Create a risk management process and cyber response plan

The SLT digital lead will work with the business professionals and IT to:

- create a simple reporting structure for cyber risks to be captured, escalated and actioned – cyber risks should be captured in the risk register and placed into a regularly tested business continuity plan

- maintain documentation and your business continuity plan in at least one or more (diverse) locations – for example, in the cloud or as a hard copy
- **flag any risks** or issues identified to the governors or trustees as part of the school or college's risk management process
- **put a cyber response plan in place**

22 Training

All staff and governors/trustees 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.

23 Review and Monitoring Arrangements

The DPO working with the DDPO is responsible for monitoring and reviewing this policy. Changes are approved by the Trust Board.

24 Links with Other Policies

This Data Protection Policy is linked to the:

- Child Protection and Safeguarding Policy
- Confidential Reporting (Whistleblowing) Code
- Data Retention Policy
- Data Security Policy
- Freedom of Information Policy & Publication Scheme.
- Artificial Intelligence Policy

Appendix 1

Data Breach Procedure

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

a. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Deputy Data Protection Officer (DDPO). The DDPO will investigate the report and determine whether a breach has occurred. To decide, the DDPO will consider whether personal data has been accidentally or unlawfully:
   (i) Lost
   (ii) Stolen
   (iii) Destroyed
   (iv) Altered
   (v) Disclosed or made available where it should not have been
   (vi) Made available to unauthorised people.

b. After investigating, the DDPO will alert the Principal and the DPO using the data breach reporting log

c. The DDPO 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)

d. The DDPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

e. In consultation with the DPO, the DDPO 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 DDPO 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:

(i) Loss of control over their data
(ii) Discrimination
(iii) Identify theft or fraud
(iv) Financial loss
(v) Unauthorised reversal of pseudonymisation (for example, key-coding)
(vi) Damage to reputation
(vii) Loss of confidentiality
(viii) 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 DDPO must notify the ICO. All breaches reported to the ICO will be notified to the chair of governors

f. The DDPO will document the decision (either way), in the DPO's data breach reporting log (online portal), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are also stored in the school's online GDPR folder

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

(i) The name and contact details of the DDPO
(ii) A description of the likely consequences of the personal data breach
(iii) 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.

h. If all the above details are not yet known, the DDPO 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 DDPO expects to have further information. The DDPO will submit the remaining information as soon as possible

i. The DDPO 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 DDPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

(i) The name and contact details of the DDPO
(ii) A description of the likely consequences of the personal data breach
(iii) 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.

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

k. The DDPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
   (i) Facts and cause
   (ii) Effects
   (iii) 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 school's Management Information System.

   The DDPO and Principal 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

The Trust 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. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

Relevant actions the Trust will take for different types of risky or sensitive personal data processed by its schools, for example sensitive information being disclosed via email (including safeguarding records):

(i) 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
(ii) Members of staff who receive personal data sent in error must alert the sender and the DDPO as soon as they become aware of the error
(iii) If the sender is unavailable or cannot recall the email for any reason, the DDPO will ask the ICT department to recall it
(iv) In any cases where the recall is unsuccessful, the DDPO 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
(v) The DDPO will ensure the Trust receive a written response from all the individuals who received the data, confirming that they have complied with this request
(vi) The DDPO will carry out an internet search to check that the information has not been made public; if it has, the Trust will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.