2019

Data Protection Policy

SMART MULTI-ACADEMY TRUST

Document Control		
Author(s):	Chris Haves	External V1.1
Updated by:		
Trustee Committee Approval	25/09/2019	
Board Approval Date	25/09/2019	
Chair of Trustees' Signature:		
Next Review Date:	September 2021	
Review Cycle:	2 Years	

Version Log

Document Title:		Data Protection Policy	
Author(s)		C.Haves	
Version number:		2.0	
Date of review:		September 2021	
Document History			
Version	**Date**	**Author**	**Note of revisions**
1.0	25/05/2018	K.Tolley	New policy
2.0	25/09/2019	C.Haves	Policy rewritten in line with School Bus Data Protection Policy template

Table of Contents

Statement of Intent

SMART Multi Academy Trust including all schools is required to keep and process certain information about its staff members', volunteers' and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The Trust may be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially children's services and other legally authorised bodies.

This policy is in place to ensure all staff and volunteers, including trustees and governors are aware of their responsibilities and outlines how the Academy Trust complies with the principles of the GDPR (section 5).

Organisational methods for keeping data secure are imperative, and the Academy Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, effective from the 25th May 2018.

1.0 Introduction

Smart Multi Academy Trust (hereinafter referred to as "the trust" regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose and vital for maintaining confidence between employees, clients and others whom we process data about, on behalf of and ourselves.

2.0 Policy Statement

2.1 This Data Protection Policy explains how the trust will meet its legal obligations concerning confidentiality and data security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) (the Legislation) which cover data security and confidentiality of personal and sensitive personal data. (A list of important defined terms in the GDPR can be found on the back pages of this policy).

1. The Trust will fully implement all aspects of the Legislation.
2. The Trust will ensure all employees and others handling personal data are aware of their obligations and rights under the Legislation.
3. The Trust will implement adequate and appropriate physical, technical and organisational measures to ensure the security of all data contained in or handled by those systems.

2.2 Compliance is evidenced in the following way:

1. On implementation of GDPR, the ICO '12 steps to take now' guide has been followed to ensure compliance in all areas. This included the appointment of a Data Protection Officer (DPO) to review processes and report to the Board of Trustees.
2. Awareness is highlighted as one of the key '12 steps to take now' by the ICO. All Smart staff have received ICO training information on implementation. Follow up information has been distributed to schools and central staff, including privacy notices, GDPR compliant policies, breach notification guidance and additional information such as GDPR FAQ document.
3. All new technologies will have DPIA's completed to ensure they are necessary and that they do not impinge on the rights of the individual. All existing processing has been evaluated in the trust Information Asset Register, where legal basis for processing has been established.

Information to support this is available on request from the DPO.

2.3 The main focus of this policy is to provide guidance about the protection, sharing and disclosure of employee and client data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or sensitive (to be called "Special Category" in the GDPR) data on behalf of the Trust.

2.4

3.0 Registration with the Information Commissioner

3.1 GDPR requires data controllers (to register with the Information Commissioner (ICO) the categories of personal data they hold and what they do with it.

3.2 The Trust is registered with the ICO under reference number ZA214693.

3.3 The Trust is a "data controller" when it decides how to use personal data. It is a "data processor" when it is directed by a third party as to how to use personal data. Further to the GDPR, both data controllers and data processors have legal obligations to safeguard personal data and are both liable if there is a breach.

4.0 Definitions of personal Data and Sensitive Personal Data

Personal data is any personally identifiable information, so this includes:

- employee data
- pupil data
- Client data
- any other personal data processed by the Trust

4.1 Examples of personal data that the Trust processes include:

- Names, addresses, emails, phone numbers and other contact information;
- Financial information;
- National insurance numbers and payroll data;
- CCTV images and photographs, video and audio recordings.

4.2 Certain types of data are identified as sensitive or "special category" and attract additional legal protection. Sensitive personal data is any data that could identify a person together with information about their:

- racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexual life;
- Commission or alleged commission of any offence;
- Information about any proceedings for any offence committed or alleged to have been committed or disposal of such proceedings or the sentence of a court in such proceedings.

5.0 Data Protection Principals (outlined in the GDPR)

5.1 We must all comply with the six data protection principles that lie at the heart of the Legislation (GDPR). The Trust fully endorses and abides by the data protection principles. Specifically, the six principles require that data is:

Principle 1: Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').

Principle 2: 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').

Principle 3: Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

Principle 4: Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified immediately ('accuracy').

Principle 5: Kept in a form that 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 GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation') (see our Information Management Policy).

Principle 6: 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').

5.2 Personal data and sensitive personal data must not be used other than for specific purposes covered by the legal basis for processing or active consent. The data subject should always know that their data is being processed and the purpose. This information is provided in our Privacy Notices.

5.3 All data collected from young people under the age of 16 (unless there are concerns about mental capacity in which case this should be extended), is not classed as sensitive personal data, but should be treated as sensitive personal data.

5.4 A record incorporating personal data can be in computerised and/or manual form. It may include such documentation as:

- Manually stored paper data e.g. employee records.
- Hand written notes.
- Letters to and from the Trust.
- Electronic records.
- Printouts.
- Photographs.
- Videos and tape recordings.

5.5 Backup data (i.e. archived data or disaster recovery records) is also subject to the Legislation.

6.0 Rights of the Individual

- **The right to be informed:** About how, why and on what basis that information is processed (see the relevant privacy notice).
- **The right of access:** To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request.
- **The right to rectification:** To have data corrected if it is inaccurate or incomplete.
- **The right to erasure:** To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten').
- **The right to restrict processing:** To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim.
- **The right to data portability:** In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.
- **The right to object to processing:** To withdraw consent to processing at any time (if applicable). To request a copy of an agreement under which personal data is transferred outside of the EEA.
- **Rights in relation to automated decision making and profiling.** To object to decisions based solely on automated processing, including profiling.

7.0 The Right of Access

7.1 Subject Access Requests (SARs): GDPR gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them irrespective of when and how they were compiled, i.e. hand written records, electronic and manual records held in a structured file, subject to certain exemptions. This is called a Subject Access Request. The Legislation treats personnel data relating to employees and clients alike.

7.2 Freedom of Information: Under the Freedom of Information Act, individuals have a right to request any recorded information held by a public authority, such as a government department, local council or state school.

The Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies
- Reports
- Financial information
- Governing information
- Funding Agreements

Classes of information specified in the publication scheme are made available quickly and easily on request.

8.0 Retention Periods

We store, retain and destroy personal information in accordance with our Information Management Policy. This policy specifies retention periods for information handled by the Trust and is available on request from the DPO.

9.0 Practical Implications

9.1 Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller. Therefore, the Trust will, through appropriate management, and strict application of criteria and controls:

- Ensure that there is a lawful basis for using personal data.
- Ensure that the use of the data is fair and will meet one of the specified conditions.
- Only process sensitive personal data where the Trust has obtained the individual's explicit consent; unless an exemption or lawful basis applies.
- Only process sensitive personal data, if it is necessary for the Trust to use it.
- Explain to individuals, at the time their personal data is collected, how that information will be used (within our Privacy Notices).
- Only obtain and use personal data for those purposes that are known to the individual.
- Only process personal data for the purpose for which it was given (where consent has been sought). If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is relevant to the Trust.
- Keep personal data accurate and up to date.
- Only keep personal data for as long as is necessary (see our Information Management Policy).
- Always adhere to our Subject Access Request Procedure and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving bulk information with exception of core administrative emails such as renewals. The Trust will always suppress the details of individuals who have opted out of receiving information (e.g. marketing).
- Will always give an option to "opt in" when consent is needed to process personal data unless there is a statutory/ legal exemption.
- Take appropriate technical and organisational security measures to safeguard personal data.

9.2 In addition, the Trust will ensure that:

- An employee is appointed as the Data Protection Officer with specific responsibility for Data Protection in the Trust (see below for roles and responsibilities).
- Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice.
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are promptly

and courteously dealt with.

- Methods of handling personal data and sensitive personal data are clearly described in polices and guidance.
- A review and audit of data protection arrangements is undertaken annually.
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Data Protection Officer and relevant directors.
- Formal written data processing agreements are in place before any personal data and sensitive personal data is transferred to a third party.

9.3 The Trust understands that recording images of identifiable individuals constitutes as processing personal information. All processing is in line with data protection principles.

9.4 CCTV cameras, recording equipment and associated information is managed in line with the Trusts CCTV Policy (available on request from the DPO).

9.5 All photography within the Trust is managed in line with the Trusts photography policy (available on request from the DPO).

10.0 Information Security

10.1 The Trust will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

10.2 All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy. Further responsibilities are outlined in the Roles and Responsibilities section.

10.3 The Trust will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

10.4 Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

10.5 Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

10.6 Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

- Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

- Availability means that authorised users can access the personal data when they need it for authorised purposes.

10.7 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Trust has implemented and maintains in accordance with the GDPR and DPA.

10.8 Where the Trust uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the Trust
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

10.9 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

10.10 The trust holds a log of suppliers and their associated privacy notices and relevant GDPR compliance documents.

11.0 Roles and Responsibilities

11.1 Maintaining confidentiality and adhering to Data Protection Legislation applies to everyone at the Trust. The Trust will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice.

11.2 Employees will receive training and information (logged in a central register) and in school and will be asked to sign to agree they reviewed relevant data protection documentation (including this policy) annually.

11.3 All employees (including agency workers), supply staff, volunteers and sub-contractors/associates have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data.
- Obtain and process personal data and sensitive personal data only for specified purposes.
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work.
- Record data correctly in both manual and electronic records.
- Ensure any personal data and sensitive personal data held is kept secure.
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party.
- Ensure personal data and sensitive personal data is sent securely; and
- Read and sign to say they have understood this policy, raising any questions to check understanding.

11.4 All Managers are responsible for:

- Determining if their operational area holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled and that the data is only used for the intended purposes(s);
- Providing clear instructions to their teams about data protection requirements and measures;
- Ensuring personal and sensitive personal data is only held for the purpose intended;
- Ensuring personal and sensitive personal data is not communicated or shared for non authorised purposes; and
- Ensuring personal and sensitive personal data is encrypted when transmitted or appropriate security measures are taken to protect when in transit or storage.

11.5 Our Data Protection Officer is Chris Haves. Responsibilities include:

- Ensuring compliance with legislation principles;
- Providing guidance and advice to employees in relation to compliance with legislative requirements;
- Auditing data protection arrangements continually.
- Reporting on any breaches of Data Protection Legislation;
- In the Data Protection Officer's absence, advice can be gained from Director of Business and Finance and general information can be found at http://www.ico.gov.uk/
- Ensuring those handling personal data are aware of their obligations by producing relevant policy, auditing the arrangements and ensuring relevant people receive training.

The DPO will report to the highest level of management at the school, which is the Headteacher and to the Chief Executive Officer and ultimately the Board of Trustees of the Academy Trust.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

11.6 Responsibility of the CEO; the CEO has overall responsibility for data protection within the Trust. The Trust has a duty to ensure that the requirements of the Legislation are upheld. The Trust relies on each of its employees and sub-contractors/associates to help in ensuring secure systems are in place to protect personal data.

11.7 Day to day data processing in school is the responsibility of the school Headteacher or Executive Head/Head of School including all responsibilities outlined in section 10.3.

11.8 The Information Commissioner Office (ICO) – The Information Commissioner's Office is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with the Legislation may lead to an investigation by the ICO which could result in serious financial or other consequences for the Trust

12.0 Breach of Policy

In the event that we fail to comply with the Legislation, an individual can complain to the DPO and/or ICO. We respectfully request that you notify the DPO or CEO in any event.

13.0 Dealing with a Data Breach

13.1 If a data breach is anticipated or identified, the person who identifies the actual or potential breach should immediately:

- Notify the relevant department manager by telephone or in person.
- Notify the Data Protection Officer by telephone or in person.
- Complete and return either the MS Word or online Breach Report Form and return to the DPO.

13.2 The Trust may have an obligation to inform the ICO, this must be done within 72 hours of the discovery of the data breach. This must be done whether the breach is identified inside or outside working hours. For out of hours breach reporting contact the DPO by email on:

DPO@smartacademies.net

13.3 Following notification of a breach, the Data Protection Officer will take the following actions as a matter of urgency:

- Implement a recovery plan, including damage limitation.
- Assess the risks associated with the breach.
- Inform the appropriate people and organisations that the breach has occurred.
- Review our response and update our information security.
- Where appropriate inform the ICO.

14.0 Policies and Procedures

This policy should be read in conjunction with the following policies and guidance (that are available from the DPO):

Policies:

- Information Management Policy
- Trust Privacy Notices
- CCTV Policy
- Freedom of Information Policy
- E-Safety Policy
- Photography Policy
- Safeguarding

Guidance:

- Document Encryption Guidance
- Dealing with a Data Subject Access Request
- Breach Report Form supporting information
- Trust GDPR and Data Protection FAQ Document

15.0 Privacy by design and Data Protection Impact Assessments

15.1 The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures that demonstrate how the Trust has considered and integrated data protection into processing activities. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Academy Trust's data protection obligations and meeting individuals' expectations of privacy.

15.2 DPIAs will allow the Academy Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation that might otherwise occur.

15.3 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data
- The use of CCTV.

The Academy Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

15.4 Where a DPIA indicates high-risk data processing, the Academy Trust will consult the ICO to

seek its opinion as to whether the processing operation complies with the GDPR. The DPO must be advised when new systems and processes involving any form of data processing are being considered. The DPO will utilise the processes determined by the ICO when reviewing all new protocols.

Glossary of Terms

Consent
Clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic) statement.

Data Subject
An individual who is the subject of personal data or sensitive personal data. This includes an employee, client or other identifiable individual.

Data Controller
A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data and sensitive personal data are, or are to be processed.

The data controller is the Trust for employee data.

Data Processor
In relation to personal data or sensitive personal data, means any person who processes that data on behalf of the data controller but is not employed by them.

Third Party
In relation to personal data or sensitive personal data, means a natural or legal person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the police or HMRC.

Personal Data
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, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Processing
Recording or holding data or carrying out any operations on that data; including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it. Essentially, if you have it, you are processing it.

Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data transmitted, stored or otherwise processed.

Subject Access Request

This is a written, signed request (which includes emails and other written formats) from an individual to see data held on them. The Data Controller must provide all such information in a readable form within 30 days of receipt of the request.