Salendine Nook High School (Academy)

Data Protection Policy (STATUTORY)

GB free to determine how to implement

Date policy written:	**November 2022**
Produced by:	**Mrs V Wood**
Approved by Governing Body:	**Finance, Staffing & General Purposes Committee 8.12.22**
Review date:	**November 2023**

TABLE OF CONTENTS

1. INTRODUCTION

1.1 This policy applies to Salendine Nook Academy Trust (hereafter referred to as the Academy) which is a registered company, limited by guarantee, in England and Wales under registration number 07883174 with a registered office at Salendine Nook High School Academy, New Hey Road, Huddersfield, West Yorkshire, HD3 4GN.

1.2 The Data Protection Act (DPA) 2018 and the UK General Data Protection Regulations (UK GDPR) provide the law which safeguards personal privacy, giving protection to individuals as to how their personal information is used. It applies to anyone who handles or has access to people's personal data.

1.3 Schools are required to have a data protection policy which must comply with the UK GDPR. This is because every school is classed as a Data Controller under the data protection legislation because they decide how personal data for which they are responsible is processed. Each school and every employee has a legal duty to protect the privacy of information relating to individuals that it processes.

1.4 The Information Commissioner as the Regulator can impose fines of up to £17.5 million for serious breaches of the UK GDPR, therefore it is imperative that the Academy and all staff comply with the legislation.

1.5 The Academy collects and uses a large amount of personal information every year about staff, pupils, parents, carers, and other individuals who come into contact with the school in order to operate. By way of example, this includes pupil records, staff records, names, and addresses of those requesting prospectuses, test marks, references, and fee collection from Local Authorities (LAs), government agencies and other bodies. In addition, there may be a legal requirement for the Academy to process personal information to ensure that it complies with statutory obligations.

1.6 The Academy may occasionally be required by law to process personal information to comply with the requirements of governmental departments and other agencies. This personal data must be dealt with properly however it is collected, recorded, and used whether on paper, held on or produced by a computer, or recorded on other material.

1.7 The Academy views the fair and lawful handling of personal data as key to its success. The Academy shall ensure that it handles all personal data fairly and lawfully.

1.8 Any failure to comply with any part of this policy may lead to disciplinary action under the Academy's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

2. PURPOSE OF THIS POLICY

2.1 The purpose of this policy is to set out how the Academy handles personal data. This policy should be read and used in conjunction with all other supporting materials listed in Appendix A.

2.2 This policy is intended to ensure that the Academy's personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded, and stored and whether it is held in paper files or electronically.

2.3 This policy sets out the obligations of the Academy with regard to data protection and the rights of people with whom it works in respect of their personal data under the UK General Data Protection Regulations (UK GDPR).

2.4 The Academy is committed to being concise, clear, and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

2.5 All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used, and ultimately deleted. All members of staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall attend regular training to ensure compliance with their responsibilities.

2.6 The Governing Board and management of the Academy are committed to compliance with all relevant legislation in respect of personal data, and the protection of the rights and freedoms of individuals whose information the Academy collects and processes.

3. SCOPE OF THIS POLICY

3.1 The Academy is a data controller under the UK GDPR. It may also be a data processor in some situations.

3.2 This policy applies to all of the Academy's personal data, processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

3.3 This policy is applicable to all personal data held by the Academy whether the information is held or accessed on company premises, on removable devices and other portable media, or accessed via mobile or home working.

3.4 This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems – paper and electronic.
- Transmission of information – e-mail, post, and telephone.
- Information systems managed and/or developed by or used by the Academy

3.5 This policy covers all information systems purchased, by or on behalf of the Academy, and any individual, directly or otherwise engaged by the organisation.

3.6 This policy applies to all directors, managers, employees, contractors, agency staff and third-party suppliers and any other individuals with access to company information.

3.7 Senior leadership and all those in managerial or supervisory roles throughout the Academy are responsible for developing and encouraging good information handling practices within the Academy.

3.8 Endorsement of this policy is mandatory at induction and should be refreshed through training annually.

3.9 More detailed specific duties with regard to the handling of data are outlined below.

4. UK GDPR CONTEXT AND DEFINITIONS PROTECTION PRINCIPLES

4.1 The EU General Data Protection Regulation (EU GDPR) supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. The EU GDPR's purpose is to protect the "rights and freedoms" of natural persons (i.e., living individuals) and to ensure that personal data is processed fairly and lawfully.

4.2 The UK General Data Protection Regulation (UK GDPR) is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679). The UK GDPR is the UK's privacy law that governs the processing of personal data within the UK.

4.3 This policy uses many terms that have specific meanings within the UK GDPR. A list of terms and an explanation of their meaning is located in Appendix B of this policy.

5. DATA PROTECTION PRINCIPLES

5.1 The Academy has established objectives for data protection and privacy.

5.2 The UK GDPR requires organisations to handle the personal data of our clients and customers in a safe, fair, and lawful manner. The Academy will ensure that it will treat all personal data fairly and lawfully and keep it secure.

5.3 To that end, the Academy fully endorses and adheres to the Data Protection Principles set out in Article 5 of the UK GDPR, whichever is applicable. The Academy's policies and procedures are designed to ensure compliance with the principles. These principles require that personal information we hold must be processed in the way set out in paragraphs 5.4 – 5.11.

5.4 Personal data must be processed lawfully, fairly, and transparently.

5.5 Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent, or legitimate interest.

5.6 Fairly – in order for processing to be fair, the controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

5.7 The UK GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

5.8 Transparently – the UK GDPR, includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

5.9 The Academy's Privacy Notice(s) can be found on its website.

5.10 The specific information that must be provided to the data subject must, as a minimum, include:

- The identity and the contact details of the controller and, if any, of the controller's representative;
- The contact details of the Data Protection Officer;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The period for which the personal data will be stored;
- The existence of each of the data subject's rights, including their rights relating to access, rectification, erasure, restriction, objection, portability, and automated decision making, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, where applicable;
- The right to withdraw consent at any time, if relevant;
- The legitimate interests of the controller, where applicable;
- The right to lodge a complaint with the supervisory authority;
- Where applicable, that the controller intends to transfer personal data to a recipient in a third country and, if so, the safeguards in place to protect the personal data;
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data (if the data is obtained directly from the data subject);
- The source of the data, if not obtained directly from the data subject and whether it came from publicly accessible sources;
- Any further information necessary to guarantee fair processing.

5.11 Personal data can only be collected for specific, explicit, and legitimate purposes.

5.12 Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

5.13 The Data Protection Manager (Director of Finance & resources), in consultation with the Data Protection Officer (DPO) as necessary, is responsible for ensuring that the Academy does not collect information that is not necessary for the purpose for which it is obtained.

5.14 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a privacy notice or link to privacy notice which has been approved by the Data Protection Manager and the DPO.

5.15 The Data Protection Manager, in consultation with the DPO as necessary, will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive.

5.16 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

5.17 At the point of collection, a verification process should be undertaken. This may take place through a verification e-mail.

5.18 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

5.19 The Data Protection Manager, in consultation with the DPO as necessary, is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

5.20 It is also the responsibility of the data subject to ensure that data held by the Academy is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

5.21 Employees/staff/students/parents/carers/others should be required to notify the Academy of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Academy to ensure that any notification regarding change of circumstances is recorded and acted upon.

5.22 The Data Protection Manager, in consultation with the DPO as necessary, is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

5.23 On at least an annual basis, the Data Protection Manager, in consultation with the DPO as necessary, will review the retention dates of all the personal data processed by the Academy, and will identify any data that is no longer required in the context of the listed purpose. This data will be securely deleted/destroyed in line with the secure destruction and disposal of personal data policy.

5.24 The Data Protection Manager, in consultation with the DPO as necessary, is responsible for responding to requests for rectification from data subjects within one calendar month, as per the Individuals' Rights Policy. This can be extended to a further two months for complex requests. If the Academy decides not to comply with the request, the Data Protection Manager (DPM), in consultation with the DPO as necessary, must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

5.25 The Data Protection Manager, in consultation with the DPO as necessary, is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

5.26 Personal data must be kept only for as long as is necessary for the purpose for which they are processed.

5.27 Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

5.28 Personal data will be retained in line with the Academy's Retention Schedule and, once its retention date is passed, it must be securely destroyed.

5.29 Records of destruction must be kept so as to satisfy the requirement to demonstrate accountability to the UK GDPR within Article 5's principles.

5.30 The Data Protection Manager, in consultation with the DPO as necessary, must specifically approve any data retention that exceeds the retention periods defined in the Retention Schedule and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

5.31 Personal data must be processed in a manner that ensures the appropriate security.

5.32 The Data Protection Manager, in consultation with the DPO as necessary, will carry out a risk assessment taking into account all the circumstances of the Academy's controlling or processing operations.

5.33 In determining appropriateness, the Data Protection Manager, in consultation with the DPO as necessary, should also consider the extent of possible damage or loss that might be caused to individuals (e.g., staff or customers) if a security breach occurs, the effect of any security breach on the Academy itself, and any likely reputational damage including the possible loss of customer trust.

5.34 When assessing appropriate technical measures, the Data Protection Manager, in consultation with the DPO as necessary, will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;

- Identifying appropriate international security standards relevant to the Academy.

5.35 When assessing appropriate organisational measures, the Data Protection Manager, in consultation with the DPO as necessary, will consider the following:

5.36 The appropriate training levels throughout the Academy;

- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Where possible, staff should try to adopt a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets, as necessary;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

5.37 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

5.38 The controller must be able to demonstrate compliance with the UK GDPR, and other principles (accountability).

5.39 The GDPR includes provisions that promote accountability and governance. These complement the UK GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

5.40 The Academy will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, Data Protection Impact Assessments (DPIA), breach notification procedures and incident response plans.

5.41 It is the Academy's duty to be responsible for and able to demonstrate adherence to these principles at all times.

6. DATA SUBJECTS' RIGHTS

6.1 Data subjects have the following rights in relation to how their personal data is processed:

- The right to be informed.
- The right of access (also known as a subject access request or SAR).

- The right to rectification (to have inaccurate data corrected).
- The right to erasure (also known as the 'right to be forgotten').
- The right to restrict processing.
- The right to data portability (to have personal data provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmitted to another controller).
- The right to object, including a right to object to direct marketing.
- Rights with respect to automated decision-making and profiling.
- The right to sue for compensation if they suffer material or non-material damage as a result of any contravention of the UK GDPR.
- The right to complain to the supervisory authority - in the UK, the information commissioner's office (ICO).

6.2 The Academy ensures that data subjects may exercise these rights.

6.3 Data subjects may make data access requests as described in Subject Access Request (SAR) Policy and the Individuals' Rights Policy. This policy also describes how the Academy will ensure that its response to the data access request complies with the requirements of the UK GDPR.

6.4 Data subjects have the right to complain to the Academy in relation to the processing of their personal data and how their requests to exercise their rights were handled.

6.5 The Academy must adhere to the SAR Policy when dealing with data subject rights.

7. SECURITY

7.1 All employees/staff are responsible for ensuring that any personal data that the Academy holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Academy to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be treated with the highest security and must be kept in accordance with all policies relating to the security of personal data as listed in Appendix A of this policy.

7.3 Final approval of any policies relating to the security of personal data is the responsibility of the Data Protection Manager, in consultation with the DPO and other stakeholders, as necessary.

7.4 Communication of this policy to those affected is the responsibility of the Data Protection Manager.

7.5 Compliance and oversight is managed by the Data Protection Manager, in consultation with the DPO, as necessary.

7.6 To demonstrate ongoing compliance, the Data Protection Manager, in consultation with the DPO and other stakeholders, as necessary, are charged with conducting periodic security audits. Any user accessing the Academy's systems is subject to unannounced audit or undisclosed monitoring.

7.7 Exceptions to policies relating to the security of personal data are granted upon written approval of the Data Protection Manager, in consultation with the DPO and other stakeholders, as necessary.

7.8 The key points to recognise as relevant to information security are outlined in between paragraphs 7.3 and 9.2 of this Data Protection Policy.

7.9 Data must be secured:

- In a lockable room with controlled access;
- In a locked drawer or filing cabinet;
- If computerised, password protected in line with academy requirements.

7.10 Stored on (removable) computer media which are encrypted.

7.11 Care must be taken to ensure that PC screens and terminals are not visible except to authorised staff of the Academy. All staff are required to enter into an Acceptable Use Agreement detailed in the staff handbook before they are given access to organisational information of any sort.

7.12 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from school premises without explicit authorisation.

7.13 Personal data may only be deleted or disposed of in line with the Secure Destruction and Deletion Policy. For example, manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately and securely destroyed before disposal.

7.14 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data. Staff must be specifically authorised to process data off-site.

7.15 All technologies used within the Academy must adhere to appropriate security requirements, which includes measures to protect electronic personal data such as ensuring firewalls and anti-malware are in place.

8. DISCLOSURE OF DATA

8.1 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Data Sharing Policy.

8.2 All confidential data must be properly inventoried, with inventories being performed periodically.

8.3 The Academy must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not the disclosure of the information is relevant to, and necessary for, the conduct of the Academy's business.

8.4 All requests to disclose data must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Manager in consultation with the DPO and other relevant stakeholders, as necessary.

8.5 The Academy will not share personal data with anyone else without consent, except in certain circumstances where it may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of the Academy's staff at risk.
- There is a need to liaise with other agencies –consent will be sought as necessary before doing this.
- The Academy's suppliers or contractors need data to provide services to the Academy's staff and pupils – for example, IT companies. When doing this, the Academy will:
  - Only appoint suppliers or contractors which 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.
- 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.

8.6 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

8.7 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information should be supervised at all times.

9. RETENTION AND DISPOSAL OF DATA

9.1 The Academy shall keep personal data in a form that permits identification of data subjects for no longer than is necessary, for the purpose(s) for which the data are processed.

9.2 The Academy may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in the Retention Schedule along with the criteria used to determine this period including any statutory obligations the Academy has to retain the data.

10. CCTV, PHOTOGRAPHS AND ELECTRONIC IMAGES

10.1 The Academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. In line with these responsibilities, the Academy will also adhere to the Biometrics and Surveillance Camera Commissioner's Surveillance Camera Code of Practice.

10.2 The purpose of CCTV at the Academy is to provide monitoring systems that assist with the protection of the property, law enforcement, traffic management, community safety and the reduction of crime and disorder, thereby improving the quality of life for all pupils, staff, and visitors to the school.

10.3 The Academy uses CCTV in various locations around its premises and CCTV is only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.4 There is no requirement to ask individuals' permission to use CCTV, but the Academy has to make it clear where individuals are being recorded. Therefore, CCTV cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

10.5 The Academy will also notify all pupils, staff, and visitors of the purpose for collecting CCTV images via notice boards, letters, and e-mails in addition to the CCTV signage on the Academy's premises.

10.6 The CCTV systems at the Academy have been notified to the ICO. The registered Owner, Operator, and Data Controller of the CCTV system is the Principal of the Academy.

10.7 The general management of CCTV at the Salendine Nook High School is currently vested with the Director of Finance & Resources.

10.8 The day-to-day management of the CCTV system is the responsibility of the ICT Manager.

10.9 An approved list of school staff that have access to CCTV footage is available from the Finance & Admin Teams and is included here as Appendix C. All other staff must make a request to a member of the Senior Leadership Team (SLT).

10.10 Any requests for CCTV footage must be documented and recorded in an appropriate format. See Appendix D for an example.

10.11 If you require the CCTV to then be copied to disc/pen drive all staff must request this from a member of SLT.

10.12 Images are retained on a hard disc for a period of 10 days. Copies can be made for investigation purposes, but requests for copies must be made via the Principal and must be returned, for destruction within 24 days to the Director of Finance & Resources.

10.13 All CCTV saved footage for minor incidents will only be kept for a maximum of 28 days. CCTV footage for more serious incidents will be kept for as long as the student's behaviour record is

kept, as this will form part of that record. Once the retention period has expired, the images will be erased.

10.14 Any enquiries about the CCTV system should be directed to the DPO.

10.15 The Academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

10.16 If the Academy wishes to use images/video footage of pupils in a publication, such as a school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parents/carers of the pupil. When using photographs and videos in this way the Academy will not accompany them with any other personal information about the child, to ensure they cannot be identified.

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

10.18 Images captured by individuals for recreational/personal purposes, and videos made by parents/carers for family use, are exempt from the UK GDPR.

10.19 Processing of surveillance footage must comply with relevant guidance and legislation including:

- ICO CCTV Code of Practice.
- Surveillance Camera Commissioner's Code of Practice.
- Surveillance Camera Commissioner's Guide to the 12 Principles.
- Freedom of Information Act 2000 (FOIA).
- Regulation of Investigatory Powers Act 2000 (RIPA).
- Power of Freedoms Act 2012 (POFA).
- Human Rights Act 1998 (HRA).
- Data Protection Act 2018 (DPA).
- UK and EU General Data Protection Regulation (UK GDPR).

11. PUBLICATION SCHEME

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

- Policies and procedures.
- Annual reports.
- Financial information.

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

11.2 The Academy will not publish any personal information, including photos, on its website without the permission of the affected individual as per paragraphs 10.15 - 10.17.

11.3 When uploading information to the school website, staff should be considerate of any metadata or deletions which could be accessed in documents and images on the site.

12. INTERNATIONAL DATA TRANSFERS

12.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the UK GDPR, as 'third countries') are unlawful unless there is an appropriate level of protection for the fundamental rights of the data subjects.

12.2 If the Academy wish to transfer personal data outside of the EEA it will apply one of the following safeguards, or rely on an exception, such as an adequacy decision.

12.3 The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

12.4 Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

Lists of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

12.5 Binding Corporate Rules

The Academy may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the Academy is seeking to rely upon.

12.6 Model Contract Clauses

The Academy may adopt approved model contract clauses for the transfer of data outside of the EEA. If The Academy adopts the model contract clauses approved by the supervisory authority, there is an automatic recognition of adequacy.

12.7 Exceptions

In the absence of an adequacy decision, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

- The transfer is necessary for the performance of a contract between the data subject and the Academy, or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Academy and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise, or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12.8 Adequacy Assessment by the Academy:

If none of the above apply, the Academy may assess adequacy itself, in accordance with Article 49 but this should only be used as a last resort. This will only apply in situations where the transfers are not repetitive, only concern a limited number of data subjects, are necessary for the purposes of the Academy's compelling legitimate interests, which are not overridden by the interests or rights and freedoms of the data subject, and the Academy has assessed all the circumstances surrounding the data transfer and provided suitable safeguards with regard to the protection of personal data. In these circumstances, the Academy shall inform the supervisory authority and the data subject.

In making an assessment of adequacy, the Academy should take account of the following factors:

- The nature of the information being transferred.
- The country or territory of the origin, and final destination, of the information.
- The purpose and duration of the proposed processing operation or operations.
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations.
- The security measures that are to be taken in relation to the personal data in the overseas location.
- For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.
- The Academy should inform the supervisory authority and the data subject about the transfer.

13. ROLES AND RESPONSIBILITIES

13.1 Governing Body

The Governing Body has ultimate responsibility for the Data Protection Policy within the Academy. Implementation of, and compliance with this policy is delegated to the designated Data Protection Manager in consultation with the DPO, where necessary.

13.2 DPO Responsibility

The Data Protection Officer (DPO) has a role and job description specified in the UK GDPR. The DPO is accountable to Governing Body of the Academy for the management of personal data within the Academy and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes development and implementation of the UK GDPR, as required by this policy and security and risk management in relation to compliance with the policy.

13.3 The Data Protection Officer has overall responsibility for Data Protection and for overseeing the development, maintenance, and monitoring of the Academy's arrangements for Data Protection including:

- The development, publishing, maintenance, and administration of the Data Protection Policy;
- The provision of data protection training for staff within the Academy;
- The development of best practice guidelines; and
- The carrying out of compliance checks to ensure adherence, throughout the Academy, under the UK GDPR.

An external provider has been appointed to the role of DPO at the Academy. The DPO will operate independently. The Academy will provide sufficient resources to the DPO to enable them to meet their GDPR obligations.

14. DATA PROTECTION MANAGER

14.1 Data protection procedures will vary from department to department. It is the responsibility of the Data Protection Manager to ensure adequate and compliant procedures are developed to handle personal data and special category personal data.

14.2 This includes the responsibility to ensure that new systems or procedures used for the processing of personal and special category personal data are carried out with reference to the Data Protection Impact Assessment (DPIA) Policy and are maintained and up to date on the DPIA register.

14.3 The Data Protection Manager may delegate the day-to-day running of operational procedures, but may not delegate overall responsibility for the handling of personal data and special category personal data.

14.4 The Data Protection Manager is responsible for reviewing the Record of Processing Activities (ROPA) annually in the light of any changes to the Academy's activities and to any additional requirements identified by means of data protection impact assessments. This register needs to be available at the supervisory authority's request.

14.5 On a day-to-day basis, the Director of Finance & Resources has been allocated as the Data Protection Manager for the managing of data protection in school. This individual will have professional experience and knowledge of data protection law, particularly in relation to schools.

14.6 The Director of Finance & Resources is responsible for continuity and recovery measures are in place to ensure the security of protected data.

14.7 The Director of Finance & Resources will report to the highest level of management at the school, which is the Principal. The Principal acts as the representative of the data controller on a day-to-day basis.

15. ALL OUR PEOPLE

15.1 As an employee of the Academy, staff are subject to an obligation of confidentiality for all personal, sensitive, and commercial information processed by the Academy, and, as such, you must adhere to the UK GDPR, and all confidentiality requirements, which form part of all employee Terms and Conditions of Employment.

15.2 All staff must sign a copy of the Academy's Confidentiality and Information Declaration without exception. Employees of external organisations who are provided with access to any personal, sensitive, or commercial information processed by the Academy must sign a confidentiality agreement and/or suitable contractual arrangements to protect and indemnify the Academy against improper use.

15.3 While you are at work you may have access to information about pupils/parents/carers/other members of staff, etc. You may come in to contact with this type of information during the course of your work or simply see, hear, or read something while you are working. Circumstances may occur where you believe that a duty of care, either to the pupil/parent/carer or to the staff member overrides the duty of confidentiality. In these circumstances you must discuss the matter with your supervisor/line manager in the first instance or escalate it to the next senior manager and/or, where practicable, obtain advice from the Data Protection Manager or DPO. The discussion and outcome must be thoroughly documented and retained for future reference.

15.4 A copy of these documents must be provided to the Data Protection Manager for audit purposes. Otherwise, you must keep this information confidential.

15.5 Any unauthorised disclosure of information by a member of staff may be considered as a disciplinary offence and could be subject to the Academy's Disciplinary Procedures.

16. OUR PROCESSES/PROCEDURES AND OUR PEOPLE

16.1 Our People:

- Our People have a duty to make sure that they comply with the data protection principles, which are set out above in the Academy's Data Protection Policy.
- Individual members of staff are responsible for ensuring that all data they are holding is kept securely.
- Individual members of staff are responsible for ensuring that paper records are destroyed securely by shredding when they are no longer required, in accordance with the Academy's Retention Schedule and Secure Destruction Policy.

- Guidance can be obtained from the Data Protection Manager regarding the safe disposal of electronically stored data.
- Members of staff should also refer to and comply with the Academy's additional internal guidance on the use of personal electronic devices for work purposes.
- Before processing any personal data or special category personal data, all members of staff should consider the checklist below.

16.2 Members of staff must consider the following factors/checklist when considering collecting personal data:

- Do you really need to record the information?
- Is the information 'personal data' or 'special category personal data'?
- If it is special category personal data and is being transferred to a third party, do you have the Data Subject's explicit consent?
- Has the Data Subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the Data Subject that the data is accurate?
- Are you sure that the data is secure?
- How long will you need to keep the data for, and what is the mechanism for review /destruction?

17. MEASURE OF EFFECTIVENESS

17.1 The true measurement of how effective this policy is will be based upon:

- Number of breaches reported.
- Number of Data Subject Rights Requests received and processed.
- Time taken to process requests.
- Satisfactory completeness of request response.

18. COMPLAINTS

18.1 Subject to paragraphs 18.2 and 18.3, complaints relating to the Academy's compliance with the GDPR will be dealt with in accordance with the Academy's Complaints Policy.

18.2 Complaints relating to access to personal information or access to education records should be made to the DPO who will decide whether it is appropriate for the complaint to be dealt with through the Academy's complaints procedure. Complaints which are not appropriate to be dealt with through the school's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter.

18.3 Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 01625 5457453.

19. REVIEW

This policy will be reviewed annually or sooner if statutory requirements change by the Data Protection Officer, Director of Finance & Resources, and the Principal**.**

20. ENQUIRIES

Any enquiries in relation to this policy should be directed to the Director of Finance & Resources via the School Office **(**office@snhs.uk**)**

Further advice and information are available from the Information Commissioner's Office at www.ico.org.uk or telephone 01625 5457453.

Appendix A

This Appendix lists those supporting policies and procedures referenced to within this Data Protection Policy:

Privacy Notice

Secure Destruction Policy

Retention Schedule

Retention Policy

SAR Policy

DPIA Policy

DPIA Register

Staff Handbook

Complaints Procedure

Acceptable Use Agreement

Appendix B

The following is a list of definitions relating to UK GDPR and that are used in the policy:

- **Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.
- **Automated Processing:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular, to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.
- **Child** (Article 8): provides that where information society services are offered directly to a child, the processing of their personal data shall be lawful if the child is at least 13 years old but if they are below 13 it shall only be lawful with parental consent.
- **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, which signifies agreement to the processing of personal data relating to them.
- **Data Controller** (Article 4): The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents/carers, and staff.
- **Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.
- **Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.
- **Data subject** (Article 4): any living individual who is the subject of personal data held by an organisation.
- **Data subject consent** (Article 4): means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **EEA:** the 28 countries in the EU, and Iceland, Liechtenstein, and Norway.
- **Explicit Consent:** consent which requires a very clear and specific statement (not just action).
- **Filing system** (Article 4): any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- **General Data Protection Regulation (GDPR):** General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.
- **Material scope** (Article 2): applies to the processing of personal data wholly or partly by automated means (i.e., by computer) and to the processing other than by automated means of personal data (i.e., paper records) that form part of a filing system or are intended to form part of a filing system.
- **Personal data** (Article 4): 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. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous

data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

- **Personal data breach** (Article 4): a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- **Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
- **Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.
- **Processing** (Article 4): any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- **Processor:** A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.
- **Profiling** (Article 4): is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
- **Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
- **Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.
- **Special categories of personal data** (Article 4): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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.
- **Territorial scope** (Article 3): applies to the processing of personal data of all controllers and processors with an establishment in the UK (United Kingdom), whether or not the processing takes place in the UK. It also applies to controllers and processors outside of the UK, if they process personal data for the purposes of offering goods and/or services to data subjects in the UK and/or monitoring the behaviour of data subjects in the UK.
- **Third party** (Article 4): a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Appendix C Staff Access Rights for CCTV

Level	Title	Access
1	ICT Technical Team	Full Access and operational use
1	SLT	Full Access and operational use
2	Finance & Admin Team	Downloading, Copying & Viewing of CCTV footage
3	All Head of Year's (HoY's), all SSM's & all SSC staff	Viewing access only

ALL other staff will need to make a request to a member of SLT

Appendix D CCTV Requests Form

CCTV DATA FORM

Request to view CCTV – Date	Name	Position	Reason for Request	SLT approval	CCTV Operator	Request to copy CCTV footage – Yes/No	Format	Release of the Footage - Date	Removal of footage - Date	Footage destroyed- date agreed by D of F& R