Records Management (GDPR) Policy

This policy applies across all partner schools in the Stephen Sutton Multi-Academy Trust (SSMAT) and should be read in conjunction with the Trust's Data Protection (GDPR) Policy. These are available on the SSMAT website and are accessible from our schools' websites.

POLICY APPROVAL and REVIEW

Review date: ***Apr. '18***

Approval needed by: ***Finance, Audit and Risk Committee***

Adopted: ***Apr. '18***

Next review date: ***Apr. '20***

CONTENTS:

1. Introduction / overview

1.1 Stephen Sutton Multi-Academy Trust (SSAT) is committed to maintaining the confidentiality of its information and ensuring that all records within the Trust can only be accessed by individuals with appropriate authority. In line with the requirements of the General Data Protection Regulation (GDPR), the Trust also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were originally intended.

1.2 This policy outlines how records are stored, accessed, monitored, retained and disposed of, in order to meet statutory requirements.

1.3 This document complies with the requirements set out in the GDPR (operational from 25 May 2018). The government has confirmed that the UK's decision to leave the EU will not affect the implementation of the GDPR. This policy should be read in conjunction with the Trust's Data Protection (GDPR) Policy.

1.4 The retention periods outlined in this policy are good practice guidelines only. In consultation with the Trust, individual partner schools should ensure that they consider requirements specific to their own setting. The tables for retention periods are based on information provided by the Information Records Management Society (IRMS) and are not an exhaustive list of records that may be kept by schools.

1.5 The names of colleagues with specific responsibility for data protection, across the Trust and in partner schools, can be found in Appendix 1 of this policy.

2. Legal framework

2.1 This policy has due regard to legislation including, but not limited to:

- the General Data Protection Regulation (2016);
- the Freedom of Information Act 2000; and
- the Limitation Act 1980 (as amended by the Limitation Amendment Act 1980).

The policy also has due regard to the IRMS 'Information Management Toolkit for Schools' 2016.

3. Responsibilities

3.1 The Trust Board holds overall responsibility for this policy.

3.2 The Headteacher and Governing Body of each SSMAT partner school are responsible for managing records in line with statutory requirements and this policy.

3.3 The Trust's Data Protection Officer (DPO) is responsible for promoting compliance with this policy and informing its review on an annual basis, in conjunction with the Executive Director and the Trust's Finance, Audit and Risk Committee.

3.4 The Data Protection Lead (DPL) (at each partner school) is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and for ensuring that records are disposed of correctly.

3.5 All colleagues are responsible for supporting the DPL in ensuring that any records for which they are responsible are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

4. Management of student records

4.1 Student records are specific documents that are used throughout a student's time in the education system. They are passed on to each school that a student attends and include all personal information relating to them, including date of birth, home address and achievement data.

4.2 The following information is easily accessible from a student's record:

- Forename, surname, gender and date of birth;
- Unique Pupil Number (UPN);
- date when the file was opened;
- date when the file was closed, as appropriate;
- ethnic origin, religion and first language (where this is not English);
- preferred name(s) (as appropriate);
- position in the family (e.g. eldest sibling);
- emergency contact details and name student's doctor;
- any allergies or other medical conditions that are important to be aware of;
- names of parents, and home address(es) and telephone number(s);
- name of the school, admission number, date of admission and date of leaving, as appropriate; and
- involvement of specialist external agencies (e.g. speech and language therapist).

4.3 Student files also include:

- admissions form;
- details of any Special Educational Needs and Disabilities (SEND);
- (where a student has attended an early years setting) the record of transfer;
- Fair Processing Notice [only the most recent notice will be included];
- annual written reports to parents;
- notes relating to major incidents and accidents involving the student;
- any information relating to an Education and Healthcare (EHC) Plan and;
- any notes indicating that Child Protection disclosures and reports are held;
- any information relating to exclusions;
- any correspondence with parents or external agencies relating to major issues (e.g. mental health); and
- notes indicating that records of complaints made by parents, or the student, are held.

4.4 The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in an appropriate secure location:

- absence notes;
- parental and, as appropriate, student consent forms for educational visits, photographs and videos, etc.; and
- correspondence with parents about minor issues, e.g. minor disciplinary infringements.

4.5 Hard copies of disclosures and reports relating to Child Protection are stored in a securely locked filing cabinet in a securely locked room – a note indicating that such records are held is made in the student's main personal file.

4.6 Hard copies of complaints made by parents, or students, are stored in a file, in an appropriately secure location – a note indicating this is marked in the student's file.

4.7 Copies of accident and incident information are stored separately on each individual school's management information system and are held in line with the retention periods outlined in this policy – a note indicating this is marked on the student's file. In the event of a major accident or incident, an additional copy may be placed in the student's file

4.8 Each school ensures that no student records are altered, or amended, before transfer to the next school that the student will attend. The only exception to this is where any records placed on the student's file have a shorter retention period and may need to be removed. In such cases, a named individual will be responsible for the disposal of records and will remove these records. Where they are held, electronic records are also transferred to the student's next school.

4.9 Wherever possible, schools avoid sending student records by post. Where a student record must be sent by post, it is sent using the 'special delivery' service, with an accompanying list of the files included. The school/agency to whom the file is sent is required to sign a copy of the list and return this to the school, indicating that the files have been received. A 'postage paid' self-addressed return envelope is provided for this purpose.

5. Retention of student records and other student-related information

5.1 The table below outlines the Trust's retention periods for individual student records, together with the action that will be taken after the retention period, in line with any requirements. Electronic files and electronic copies of any other information are also destroyed, in line with the retention periods below.

Type of document / file	Retention period	Action taken at end of retention period
Admissions		
Register of admissions	Six years after the date on which the entry was made.	Information is reviewed, so the register may be kept permanently. Otherwise, disposed of securely.
Supplementary information submitted with application/appeal documentation, including religious and medical information etc. (where the admission was successful)	25 years after the student's date of birth. (Added to the student's record).	Disposed of securely.
Supplementary information submitted with application/appeal documentation, including religious and medical information etc. (where the admission was not successful)	Until the appeals process has been completed.	Disposed of securely.
Students' educational records		
Primary educational records	Whilst the student remains at the school.	Transferred to the next destination. Where this is an independent school, home-schooling or outside of the UK, the file is kept by the LA and retained for the statutory period.
Secondary educational records	25 years after the student's date of birth. (Added to the student's record).	Disposed of securely.
Public examination results	25 years after the student's date of birth. (Added to the student's record).	Disposed of securely.
Internal examination results	25 years after the student's date of birth. (Added to the student's record).	Disposed of securely.
Child Protection information (held in a separate file)	25 years after the student's date of birth. (Added to the student's record).	Disposed of securely - shredded on site.

Type of document / file	Retention period	Action taken at end of retention period
Attendance		
Attendance registers	Last date of entry on to the register, plus six years	Disposed of securely.
Authorisation of absence letters	Current academic year, plus two years	Disposed of securely.
SEND		
SEND files, reviews and Individual Education Plans (IEPs)	25 years after the student's date of birth (as stated on the student's record)	Information is reviewed and the file may be kept for longer than necessary, if it is required for the school to defend itself in a 'failure to provide sufficient education' case
Statement of SEN, maintained under Section 324 of the Education Act 1996 / EHC plan, maintained under Section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the student's date of birth (as stated on the student's record)	Disposed of securely (unless subject to a legal 'hold').
Information and advice provided to parents regarding SEND	25 years after the student's date of birth (as stated on the student's record)	Disposed of securely (unless subject to a legal 'hold').
Accessibility strategy	25 years after the student's date of birth (as stated on the student's record)	Disposed of securely (unless subject to a legal 'hold').
Curriculum-related		
Students' marked examination scripts	Until the appeals / validation process has been completed	Disposed of securely.
Student-level value-added / contextual data	Current academic year, plus six years	Disposed of securely.
Students' work	Retained for the current academic year, plus one year (where not already returned to students).	Disposed of securely.

Type of document / file	Retention period	Action taken at end of retention period
Extra-curricular activities		
Parental consent forms for school trips (where no major incident occurred)	Until the conclusion of the trip.	Disposed of securely.
Parental consent forms for school trips (where a major incident occurred)	25 years after the student's date of birth, as shown on the student's record. [Permission slips for all students on the trip will be held to show that correct procedures had been followed].	Disposed of securely.
'Walking bus' registers	Three years from the date of the register being taken.	Disposed of securely.

6. Retention of staff records

6.1 The table below outlines the Trust's retention period for staff records and the action that is taken after the retention period, in line with any requirements. Electronic files and electronic copies of information are also destroyed, in line with the retention periods below.

Type of document / file	Retention period	Action taken at end of retention period
Operational		
Staff members' personal files	Termination of employment, plus six years	Disposed of securely – shredded on site.
Timesheets	Current academic year, plus six years	Disposed of securely.
Annual appraisal records	Current academic year, plus six years	Disposed of securely.
Recruitment		
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Disposed of securely.
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the colleague's personal file and other information retained for six months.	Disposed of securely.

Type of document / file	Retention period	Action taken at end of retention period
Operational		
Proof of identity / address and evidence to work in the UK, as part of the Enhanced DBS check	Documentary evidence checked and copied. Original documents handed back immediately. Copies kept in personal file (for the duration of time that the personal file is kept, i.e. termination of employment, plus six years).	Copies disposed of securely – shredded on site with other contents of personal file.
Change of address / name / other personal details	Documentary evidence checked and copied. Original documents handed back immediately. Copies kept in personal file (for the duration of time that the personal file is kept, i.e. termination of employment, plus six years).	Copies disposed of securely – shredded on site with other contents of personal file.
Disciplinary and grievance procedures		
Child Protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer. [Where a formal process has been followed, leading to a judgement that an allegation is malicious, the details relating to this allegation are removed from the personal file].	Reviewed and disposed of securely – shredded on site.
First written warning – Stage 1	Date of warning, plus six months.	Removed from staff personal file and disposed of securely – shredded on site.
Final written warning – Stage 2	Date of warning, plus 12 months.	Removed from staff personal file and disposed of securely – shredded on site.

7. Retention of governance and management records

7.1 The table below outlines the Trust's retention periods for governance and management records, and the action that is taken after the retention period, in line with any requirements. Electronic copies of any information and files is also destroyed, in line with the retention periods below.

Type of document / file	Retention period	Action taken at end of retention period
Governing Body / Trust Board		
Minutes of Governing Body / Trust Board meetings	Permanent	N/A
Reports presented to the Governing Body / Trust Board that include data that identifies individuals.	Current academic year, plus six years.	Disposed of securely – shredded on site.
Older versions of policies	Current academic year, plus six years.	Disposed of securely.
Records relating to complaints dealt with by the Governing Body / Trust Board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes and then disposed of securely – shredded on site.
Headteacher and Senior Leadership Team (SLT)		
Minutes of SLT meetings and the meetings of internal administrative bodies	Date of the meeting, plus six years.	Reviewed and securely disposed of
Management reports (internally or externally generated), e.g. school census	Date of the report, plus six years.	Reviewed and disposed of securely.
Records created by the Headteacher / SLT and other colleagues with administrative responsibilities	Current academic year, plus six years.	Reviewed and disposed of securely.
Copies of correspondence held anywhere other than in staff personal files that identifies individuals.	Date of correspondence, plus six years.	Reviewed and disposed of securely.
Performance analyses and action plans / training plans (where these identify individual staff)	Duration of the plan, plus six years.	Disposed of securely.

8. Retention of Health and Safety records

8.1 The table below outlines the Trust's retention periods for health and safety records, and the action that is taken after the retention period, in line with any requirements. Electronic copies of any information and files is also destroyed, in line with the retention periods below.

Type of document / file	Retention period	Action taken at end of retention period
Health and Safety		
Health and Safety risk assessments	Duration of risk assessment, plus six years.	Disposed of securely.
Records relating to accidents and injuries to staff at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied.	Disposed of securely.
Accident reporting – adults / members of the community	Date of the incident, plus six years.	Disposed of securely.
Accident reporting – students	25 years after the student's date of birth, on the student's record.	Disposed of securely.
Control of substances hazardous to health (inventory / risk assessments)	Current academic year, plus 40 years.	Disposed of securely.
Information relating to areas where colleagues and other persons are likely to come into contact with asbestos	Date of last action, plus 40 years.	Disposed of securely.
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years.	Disposed of securely.
Fire precautions (log books)	Current academic year, plus six years.	Disposed of securely.

9. Retention of financial records

9.1 The table below outlines the Trust's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of document / file	Retention period	Action taken at end of retention period
Payroll / pensions		
Payroll records	Current academic year, plus six years	Disposed of securely.
Type of document / file	**Retention period**	**Action taken at end of retention period**
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years.	Transferred, as appropriate, on closure and then disposed of securely, 40 years later.
Asset management		
Inventories of furniture and equipment	Current academic year, plus six years.	Disposed of securely.
Accounts and statements (including budget management)		
Annual accounts	Current academic year, plus six years.	Disposed of (against common standards).
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years.	Disposed of securely.
Records relating to the collection and banking of monies	Current financial year, plus six years.	Disposed of securely.
Records relating to the identification and collection of debt	Current financial year, plus six years.	Disposed of securely.
Contract management		
All records relating to the management of contracts (under both seal and signature)	Last payment on the contract, plus six years.	Disposed of securely.
School fund		
Cheque books, paying in books, ledgers, invoices, receipts and bank statements	Current academic year, plus six years.	Disposed of securely.

Free school meals		
Free school meals registers	Current academic year, plus six years.	Disposed of securely.

10. Retention of other school records

10.1 The table below outlines the Trust's retention periods for other records, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files are also destroyed, in line with the retention periods below.

Type of document / file	Retention period	Action taken at end of retention period
Property management		
Title deeds of properties belonging to the Trust	Permanent	Transferred to new owners if / when building is leased or sold.
Plans of property belonging to the Trust	For as long as the building belongs to the Trust.	Transferred to new owners if / when building is leased or sold.
Leases of property leased by, or to, the Trust / school	Expiry of lease, plus six years.	Disposed of securely.
Records relating to the letting of school premises	Current financial year, plus six years.	Disposed of securely.
Maintenance		
All records relating to the maintenance of Trust / school premises	Current academic year, plus six years.	Disposed of securely.
Operational administration		
Visitors' books and signing-in sheets	Current academic year, plus six years.	Reviewed and then disposed of securely.
	Biometric data–staff/ students	
Any biometric data that is stored, and used, for an automated biometric recognition system.	Only to be retained for as long as it is being used (and consent is in place).	Disposed of securely.

11. Storing and protecting information

11.1 Each school's GDPR Lead undertakes an annual risk analysis to identify which records are vitally important to the management of the school and the Trust and these records are stored in the most secure manner.

11.2 Each school conducts a 'back-up' of information, in line with agreed procedures, to ensure that, in the event of a security breach (e.g. a virus), all data can still be accessed, and to prevent any loss or theft of data. Where possible, 'backed-up' information is stored off the school premises, using a central back-up service operated from a remote site.

11.3 Confidential paper records are kept in a locked filing cabinet, drawer or safe, with appropriately restricted access. They are not left unattended or in clear view when held in a location with general access.

11.4 Digital data is encrypted, whilst in storage. No personally identifiable data remains on generally accessible or multi-user machines, once a user logs out.

11.5 Personal information is not stored on any form of removable storage (e.g. CD, DVD, USB memory stick, memory card, external hard drive or 'Cloud' storage).

11.6 All electronic devices are protected, using either password, personal identification number (PIN) or biometric recognition, in order to protect the information on the device, in case of theft.

11.7 Where possible, the Trust and its schools make use of technology that allows for electronic devices to be remotely controlled, secured or data deleted, in case of theft.

11.8 Staff do not use their personal laptops or computers for school purposes.

11.9 All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password in line, with agreed procedures.

11.10 External emails containing sensitive or confidential information are marked 'confidential' in the subject bar, by the sender, and are thereby automatically encrypted. Recipients are required to generate a single use code, in order to access the contents of the message, which is automatically deleted after 30 days.

11.11 Circular emails to parents are sent blind carbon copy (bcc), so that email addresses are not disclosed to other recipients.

11.12 When sending confidential information by fax, colleagues check that the fax address is correct for the recipient before sending.

11.13 Where, in line with GDPR policy and protocol, personal information (that could be considered private or confidential) is taken off the premises (either in electronic or paper format), colleagues take extra care to follow the same procedures for security (e.g. keeping devices under lock and key) as they would on the school premises. The person taking the information from the school premises accepts full responsibility for the security of the data.

11.14 Before sharing data, colleagues ensure that:

- they have the consent of the data subjects to share it;

- adequate security is in place to protect it; and
- the data recipient has been outlined in a Privacy Notice.

11.15 Colleagues implement a 'clear desk policy', in order to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information is stored in a securely locked filing cabinet, drawer or safe with restricted access. Visitors are not allowed access to confidential or personal information. Visitors to areas that contain sensitive information are supervised at all times.

11.16 The physical security of the Trust's buildings and storage systems, and access to them, is reviewed termly by the GDPR Lead, in conjunction with the Site Manager / Business Manager. Where an increased risk of vandalism, burglary or theft is identified, this is reported to the Headteacher and extra measures are taken to ensure that secure data storage is in place.

11.17 The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

11.18 The GDPR Lead is responsible for ensuring that continuity and recovery measures are in place to ensure the security of protected data.

12. Information audit

12.1 The Trust conducts information audits, on an annual basis, against all information held by each school, in order to review the nature of the information that each school is holding, receiving and using, and to ensure that this is correctly managed, in accordance with the GDPR. These audits cover:

- paper documents and records;
- electronic documents and records;
- databases;
- sound recordings; and
- video and photographic records.

12.2 The information audit may be completed in a number of ways, including, but not limited to interviews with, and/or questionnaires completed by, colleagues with key responsibilities. These approaches are designed to identify the information held and the flow of information around the records management system.

12.3 The GDPR Lead is responsible for completing the information audit, which will include:

- the school's (and Trust's) data needs;
- the information required to meet those needs;
- the format(s) in which data is stored;
- how long data is, and needs to be, kept for; and
- the status of vitally important records and any protective marking.

12.4 The GDPR Lead consults with colleagues involved in the information audit process to ensure that the information is accurate. Once it has been confirmed that the information is accurate, the GDPR Lead will record all details on the Information Asset Register. The

information displayed on the Information Asset Register will be shared with the Executive Director, the Trust Board and each school's Headteacher.

13. Disposal of data

13.1 Where the disposal of information is identified as 'standard disposal', this is done through recycling, appropriate to the form of the information, e.g. paper recycling, electronic recycling.

13.2 Where the disposal of information is identified as 'secure disposal', this is achieved through shredding or pulping, for hard copy; electronic information is 'scrubbed clean' and, where possible, cut. The GDPR Lead keeps a record of all files that have been destroyed.

13.3 Where the disposal action is indicated as 'review before it is disposed', the GDPR Lead reviews the information against its administrative value. Where it is decided that the information should be kept, for its administrative value, the GDPR Lead keeps a record of this. Where, after the review, it is determined that the data should be disposed of, it is destroyed, in accordance with the disposal action outlined in this policy.

13.4 Where information is kept, for administrative purposes, the DP Lead reviews the information again after a period of three years and conducts the same process. However, where information must be kept permanently, this information is exempt from the normal review procedures

Stuart Jones/Sharon Thorp; 03/05/18

Appendix 1 - Staff with specific GDPR-related responsibilities – by name

Stephen Sutton Multi-Academy Trust Core Team

GDPR-related role	*Job title*	*Name*
Data Controller	Executive Director	Stuart Jones
Data Protection Officer (DPO)	Trust Business Manager	Sharon Thorp

Chase Terrace Technology College

GDPR-related role	*Job title*	*Name*
Overall responsibility for GDPR implementation in CTTC	Headteacher	Tim Chamberlin
Data Protection Lead (DPL)	Business Manager (CTTC)	Selina Morgan