ST TERESA of CALCUTTA
Catholic Academy Trust

Data Retention Policy

Policy Level	Trust/Statutory	Ref No	ADM07
Approved by	CSEL	Approved date	January 4th 2023
Responsibility	DPO	Next review	Autumn 2024
Published location	STOC Shared Policy Folder	Date Issued	Spring 2023
Version number	2	Author	CIO

Contents

Section	Page
1.0 Policy Statement	1
2.0 Legal Framework	1
3.0 Roles and Responsibilities	2
4.0 Management of Pupil Records	2
5.0 Retention of Pupil Records and Other Pupil Related Information	4
6.0 Retention of Staff Records	11
7.0 Retention of Senior Leadership and Management Records	13
8.0 Retention of Health and Safety Records	14
9.0 Retention of Financial Records	15
10.0 Retention of other School Records	18
11.0 Retention of Emails	19
12.0 Storing and Protecting Information	19
13.0 Accessing Information	20
14.0 Digital Continuity Statement	22
15.0 Information Audit	22
16.0 Disposal of Data	22

1.0 Policy Statement

1.1 The Trust's contact details are as follows:

St Teresa of Calcutta Catholic Academy Trust (STOC)

Imperial House

Hornby Street

Bury

BL9 5BN

admin@stoccat.org.uk

1.2 The Trust's Data Protection Officer's contact details are as follows:

Jennifer Bonson

St Teresa of Calcutta Catholic Academy Trust (STOC)

Imperial House

Hornby Street

Bury

BL9 5BN

jbonson@stoccat.org.uk

1.3 The Trust is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to the appropriate individuals. In line with the requirements of UK 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 intended.

1.4 The Trust has created this policy to outline how records are stored, accessed, monitored, retained and disposed of to meet school's statutory requirements.

1.5 This document complies with the requirements set out in the UK GDPR and Data Protection Act 2018.

2.0 Legal Framework

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

- UK General Data Protection Regulation (GDPR)
- EU GDPR
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018

2.2 This policy also has due regard to the following guidance:

- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2021) 'Careers guidance and access for education and training providers'
- ESFA (2022) 'Record keeping and retention information for academies and academy trusts'
- Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools'
- IRMS (2019) 'Academies Toolkit'

2.3 This policy will be implemented in accordance with the following school policies and procedures:

- Data Protection Policy
- Data and Cyber-security Breach Prevention and Management Plan
- Disposal of Records Log
- Archived Files Log
- Data Asset Register

3.0 Roles and Responsibilities

3.1 Each school within the Trust has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements and the retention schedule provided in this policy.

3.2 The headteacher holds the overall responsibility for this policy and for ensuring it is implemented correctly.

3.3 The DPO is responsible for:

- The management of records at the school.
- Promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the headteacher.
- Ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of safely and correctly.

3.4 All staff members are responsible for ensuring that any records they are responsible for (including emails) are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

4.0 Management of Pupil Records

4.1 Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and include all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievements.

4.2 The following information is stored on the front of a pupil record, and will be easily accessible:

- Forename, surname, and date of birth
- Unique pupil number
- Note of the date when the file was opened

4.3 The following information is stored inside the front cover of a pupil record, and will be easily accessible:

- Any preferred names

- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of people with parental responsibility, including their home address(es) and telephone number(s)
- Any other agency involvement, e.g. speech and language therapist
- Reference to any other linked files

4.4 The following information is stored in a pupil record, and will be easily accessible:

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Data collection or data checking form
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil
- Any information about an EHC plan and support offered in relation to the EHC plan
- Medical information relevant to the pupil's on-going education and behaviour
- Any notes indicating child protection disclosures and reports
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil
- Examination results – pupil copy
- SATs results

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

- Attendance registers and information
- Absence notes and correspondence
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Accident forms – forms about major accidents will be recorded on the pupil record
- Consent to administer medication and administration records
- Copies of pupil birth certificates, passports etc.
- Correspondence with parents about minor issues, e.g. behaviour
- Pupil work
- Previous data collection forms that have been superseded

4.6 Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet – a note indicating this is marked on the pupil's file.

4.7 Hard copies of complaints made by parents or pupils are stored in a file in the headteacher's office – a note indicating this is marked on the pupil's file.

4.8 Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy – a note indicating this is

marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

4.9 The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend. The only exception is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the DPO will remove these records.

4.10 Electronic records relating to a pupil's record will also be transferred to the pupils' next school.

4.11 **[Primary schools]** The school will not keep any copies of information stored within a pupil's record unless there is ongoing legal action at the time during which the pupil leaves the school. The responsibility for these records will then transfer to the next school that the pupil attends.

4.12 **[Secondary schools and Sixth-Form Colleges]** If any pupil attends the school until statutory school leaving age, the school will keep the pupil's records until the pupil reaches the age of 25 years.

4.13 The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

5.0 Retention of Pupil Records and Other Pupil Related Information

5.1 The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.

5.2 Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of File	Retention Period	Action Taken after Retention Period Ends
Personal Identifiers, Contacts and Personal Characteristics		
Images used for identification purposes.	For the duration of the event/activity, or whilst the student remains at the school, whichever is less, plus one month.	Data is securely disposed of.
Images used in displays in the school.	Whilst the student is at the school.	Data is securely disposed of.
Images used for marketing purposes, social media or other.	In line with the consent period.	Data is securely disposed of.
Biometric Data.	For the duration of the event/activity, or whilst the student remains at the school, whichever is less, plus one month.	Data is securely disposed of.

Postcodes, Names and Characteristics.	Whilst the student is at the school, plus five years.	Data is securely disposed of.
House Number and Road.	For the duration of the event/activity, plus one month.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Admissions		
Register of Admissions.	Whilst the student remains at the school, plus one year.	Information is reviewed and the register may be kept permanently.
Admissions Appeals.	Whilst the student remains at the school, plus five years.	Data is securely disposed of.
[Secondary schools only] Secondary School Admissions.	Whilst the student remains at the school, plus one year.	Data is securely disposed of.
Proof of Address (supplied as part of the admissions process).	Whilst the student remains at the school, plus one year.	Data is securely disposed of.
Supplementary information submitted, including religious and medical information etc. (where the admission was successful).	Whilst the student remains at the school, plus one year.	Data is securely disposed of.
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful).	Whilst the student remains at the school, plus five years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Pupils' Educational Records		
[Primary Schools only] Students' Educational Records.	Whilst the student remains at the school.	Transferred to the next destination – if this is an independent school, home-Schooling or outside of the UK, the file will be kept by the Trust and retained for the statutory period.

[Secondary Schools only] Students' Educational Records.	25 years after the student's date of birth, with their personal data removed.	Data is securely disposed of.
Public Examination Results.	Added to the student's record and transferred to next school. Copies with students' names are held whilst the student is at the school, plus five years. Copies with students' names removed are held for 25 years after the student's date of birth.	Returned to the examination board.
Internal Examination Results.	Added to the student's record and transferred to next school. Copies with the student's personal data are held whilst the pupil is at the school, plus five years. Copies with personal data removed are held for 25 years after the student's date of birth.	Data is securely disposed of.
Behaviour Records.	Added to the student's record and transferred to the next school. Copies are held whilst the student is at the school, plus one year.	Data is securely disposed of.
Exclusion Records.	Added to the student's record and transferred to the next school.	Data is securely disposed of.

	Copies are held whilst the student is at the school, plus one year.	
Child Protection Information held on a Student's Record.	Stored in a sealed envelope or securely electronically for the same length of time as the student's record.	Data is securely disposed of – shredded.
Child Protection Records held in a Separate File.	25 years after the student's date of birth.	Data is securely disposed of – shredded.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Attendance		
Attendance Registers.	Whilst the student remains at the school, plus one year. Non-identifiable summary statistics are held after the initial retention period for 25 years after the student's date of birth.	Data is securely disposed of.
Letters Authorising Absence.	Whilst the student remains at the school, plus one year. Non-identifiable summary statistics are held after the initial retention period for 25 years after the student's date of birth.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Medical Information and Administration		
Permission slips.	For the duration of the period that medication is given, plus one month.	Data is securely disposed of.

Medical Conditions – ongoing management.	Added to the student's record and transferred to the next school. Copies are held whilst the student is at the school, plus one year.	Data is securely disposed of.
Medical Incidents that have a behavioural or safeguarding influence.	Added to the student's record and transferred to the next school. Copies held whilst the student is at the school, plus 25 years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
SEND		
SEND files, reviews and individual education plans.	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 themselves in a 'failure to provide sufficient education' case.
An 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).	Data is securely disposed of, unless it is 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).	Data is securely disposed of, unless it is subject to a legal hold.
Accessibility Strategy.	25 years after the pupil's date of birth (as stated on the student's record).	Data is securely disposed of, unless it is subject to a legal hold.

Type of File	Retention Period	Action Taken after Retention Period Ends
Curriculum Management		
SATs Results.	25 years after the student's date of birth (as stated on the student's record).	Data is securely disposed of.
Examination Papers.	Until the appeals/validation process has been completed.	Data is securely disposed of.
Published Admission Number (PAN) Reports.	Current academic year, plus six years.	Data is securely disposed of.
Valued Added and Contextual Data.	Current academic year, plus six years.	Data is securely disposed of.
Self-Evaluation Forms.	Current academic year, plus six years.	Data is securely disposed of.
Pupils' Work.	Returned to students at the end of the academic year, or retained for the current academic year, plus one year.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Extra-Curricular Activities		
Field file – information taken on school trips.	Until the conclusion of the trip, plus one month. Where a minor incident occurs, field files are added to the core system as appropriate.	Data is securely disposed of.
Financial Information relating to school trips.	Whilst the student remains at the school, plus one year.	Data is securely disposed of.
Parental consent forms for school trips where no major incident occurred.	Until the conclusion of the trip.	Data is securely disposed of.

Parental consent forms for school trips where a major incident occurred.	25 years after the student's date of birth on the student's record (permission slips of all students on the trip will also be held to show that the rules had been followed for all students)	Data is securely disposed of.
Walking Bus Registers.	Three years from the date of the register being taken.	Data is securely disposed of.
Educational visitors in the school – sharing of personal information.	Until the conclusion of the visit, plus one month.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Family Liaison Officers and Home-School Liaison Assistants		
Day books.	Current academic year, plus two years.	Reviewed and destroyed if no longer required.
Reports for outside agencies.	Duration of the student's time at the school.	Data is securely disposed of.
Referral Forms.	Whilst the referral is current.	Data is securely disposed of.
Contact Data Sheets.	Current academic year.	Reviewed and destroyed if no longer active.
Contact Database Entries.	Current academic year.	Reviewed and destroyed if no longer required.
Group Registers.	Current academic year, plus two years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Catering and Free School Meal Management		
Meal Administration.	Whilst the student is at the school, plus one year.	Data is securely disposed of.

Meal Eligibility.	Whilst the student is at the school, plus five years.	Data is securely disposed of.

6.0 Retention of Staff Records

6.1 The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

6.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of File	Retention period	Action Taken after Retention Period Ends
Operational		
Staff members' Personal File.	Termination of employment, plus six years.	Data is securely disposed of.
Timesheets.	Current academic year, plus six years.	Data is securely disposed of.
Annual appraisal and assessment records.	Current academic year, plus five years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Recruitment		
Records relating to the appointment of a new headteacher.	Date of appointment, plus six years.	Data is securely disposed of.
Records relating to the appointment of new members of staff (unsuccessful candidates).	Date of appointment of successful candidate, plus six months.	Data is securely disposed of.
Records relating to the appointment of new members of staff (successful candidates).	Relevant information added to the member of staff's personal file and other information retained for six months.	Data is securely disposed of.
DBS certificates.	Up to six months.	Data is securely disposed of.
Proof of identify as part of the enhanced DBS check.	After identity has been proven.	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a

		copy this will be placed on the staff member's personal file, if not, data is securely disposed of.
Evidence of right to work in the UK.	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
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. If allegations are malicious, they are removed from personal files.	Data is reviewed and securely disposed of – shredded.
Any Type of Formal Warning.	The warning will remain active for 6 months and it should be disregarded for disciplinary purposes after this period (Discipline Policy).	Detail of the warning should remain in place for the length of the life of the file +6 years (if they leave) as per the other documentation. After this, it should be securely disposed of.
Records relating to unproven incidents.	Conclusion of the case, unless the incident is child protection related and is disposed of as above.	Data is securely disposed of.

7.0 Retention of Senior Leadership and Management Records

7.1 The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

7.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of File	Retention Period	Action Taken after Retention Period Ends
Local Governing Boards		
Agendas for LGB Meetings.	One copy alongside the original set of minutes – all others disposed of without retention.	Data is securely disposed of.
Original, signed copies of the minutes of LGB meetings.	Permanent.	N/A.
Inspection copies of the minutes of LGB meetings.	Date of meeting, plus three years.	Shredded if they contain any sensitive and personal information.
Reports presented to the LGB.	Minimum of six years, unless they refer to individual reports – these are kept permanently.	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes.
Instruments of Governance, including articles of association.	Permanent	If unable to store, these will be provided to the county archives service.
Action plans created and administered by the LGB.	Duration of the action plan, plus three years	Data is securely disposed of.
Policy documents created and administered by the LGB.	Duration of the policy, plus three years.	Data is securely disposed of.
Records relating to complaints dealt with by the LGB.	Date of the resolution of the complaint, plus a minimum of six years.	Reviewed for further retention in case of contentious disputes, then securely disposed of.

Annual Reports.	Date of report, plus 10 years.	Data is securely disposed of.
Proposals concerning changing the status of the school.	Date proposal accepted or declined, plus three years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Headteacher and Senior Leadership Team (SLT)		
Minutes of SLT meetings and the meetings of other internal administrative bodies.	Date of the meeting, plus three years.	Reviewed and securely disposed of.
Reports created by the Headteacher or SLT.	Date of the report, plus a minimum of three years.	Reviewed and securely disposed of.
Records created by the Headteacher, deputy Headteacher, heads of year and other members of staff with administrative responsibilities.	Current academic year, plus six years.	Reviewed and securely disposed of.
Correspondence created by the Headteacher, deputy Headteacher, heads of year and other members of staff with administrative responsibilities.	Date of correspondence, plus three years.	Reviewed and securely disposed of.
Professional development plan.	Duration of the plan, plus six years.	Data is securely disposed of.
School development plan.	Duration of the plan, plus three years.	Data is securely disposed of.

8.0 Retention of Health and Safety Records

8.1 The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

8.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of File	Retention Period	Action Taken after Retention Period Ends
Health and Safety		
Health and Safety Policy Statements.	Duration of policy, plus three years.	Data is securely disposed of.
Health and Safety Risk Assessments.	Duration of risk assessment, plus three years.	Data is securely disposed of.
Records relating to Accidents and Injuries at work.	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied.	Data is securely disposed of.
Accident Reporting – Adults.	Date of the incident, plus six years.	Data is securely disposed of.
Accident Reporting – Pupils.	25 years after the pupil's date of birth, on the pupil's record.	Data is securely disposed of.
Control of Substances Hazardous to Health.	Current academic year, plus 40 years.	Data is securely disposed of.
Information relating to areas where employees and persons are likely to come into contact with asbestos.	Date of last action, plus 40 years.	Data is securely disposed of.
Information relating to areas where employees and persons are likely to come into contact with radiation.	Date of last action, plus 50 years.	Data is securely disposed of.

9.0 Retention of Financial Records

9.1 The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

9.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action Taken after Retention Period Ends
Payroll Pensions		
Maternity Pay Records	Current academic year, plus three years.	Data is securely disposed of.
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995.	Current academic year, plus six years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Risk Management and Insurance		
Employer's Liability Insurance Certificate.	Closure of the school, plus 40 years.	Data is securely disposed of.
Asset Management		
Inventories of Furniture and Equipment.	Current academic year, plus six years.	Data is securely disposed of.
Burglary, Theft and Vandalism Report forms.	Current academic year, plus six years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Accounts and Statements including Budget Management		
Annual Accounts	Current academic year, plus six years.	Disposed of against common standards.
Loans and Grants managed by the school.	Date of last payment, plus 12 years.	Information is reviewed then securely disposed of.
All records relating to the creation and management of budgets.	Duration of the budget, plus three years.	Data is securely disposed of.
Invoices, receipts, order books, requisitions and delivery notices.	Current financial year, plus six years.	Data is securely disposed of.
Records relating to the collection and banking of monies.	Current financial year, plus six years.	Data is securely disposed of.

Records relating to the identification and collection of debt.	Current financial year, plus six years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Contract Management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years.	Data is securely disposed of.
All records relating to the management of contracts under signature	Last payment on the contract, plus six years.	Data is securely disposed of.
All records relating to the monitoring of contracts.	Current academic year, plus two years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
School Fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books.	Current academic year, plus six years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
School Meals		
Free School Meals Registers.	Current academic year, plus six years.	Data is securely disposed of.
Academy meals registers	Current academic year, plus three years	Securely disposed of
Academy meals summary sheets	Current academic year, plus three years	Securely disposed of

10.0 Retention of other School Records

10.1 The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

10.2 Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of File	Retention Period	Action Taken after Retention Period Ends
Property Management		
Plans of property belonging to the school.	For as long as the building belongs to the school.	Transferred to new owners if the building is leased or sold.
Leases of property leased by or to the school.	Expiry of lease, plus six years.	Data is securely disposed of.
Records relating to the letting of school premises.	Current financial year, plus six years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Maintenance		
All records relating to the maintenance of the school carried out by contractors.	Current academic year, plus six years.	Data is securely disposed of.
All records relating to the maintenance of the school carried out by school employees.	Current academic year, plus six years.	Data is securely disposed of.
Type of File	**Retention Period**	**Action Taken after Retention Period Ends**
Operational Administration		
General file series.	Current academic year, plus five years.	Reviewed and securely disposed of.
Records relating to the creation and publication of the school brochure and/or prospectus.	Current academic year, plus three years.	Disposed of against common standards.
Records relating to the creation and distribution of circulars to staff, parents or pupils.	Current academic year, plus one year.	Disposed of against common standards.
Newsletters and other items with short operational use.	Current academic year plus one year.	Disposed of against common standards.
Visitors' books and signing-in sheets.	Current academic year, plus six years.	Reviewed then securely disposed of.

Records relating to the creation and management of parent-teacher associations and/or old pupil associations.	Current academic year, plus six years.	Reviewed then securely disposed of.

11.0 Retention of Emails

11.1 Group email addresses will have an assigned member of staff who takes responsibility for managing the account and ensuring the correct disposal of all sent and received emails. All staff members with an email account will be responsible for managing their inbox.

11.2 Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties, so all relevant emails, e.g. invoices, will be retained for at least 12 months. Invoices received and sent in emails will be printed off and retained in accordance with this policy.

11.3 The school's expectations of staff members in relation to their overall conduct when sending and receiving emails is addressed in the Trust's communication policy. All emails will be automatically deleted after 2 years, unless stated otherwise.

11.4 Correspondence created by the SLT and other members of staff with administrative responsibilities will be retained for three years before being reviewed and, if necessary, securely disposed of.

11.5 Staff members will review and delete any emails they no longer require at the end of every term.

11.6 Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives. Staff members will be aware that the emails they send could be required to fulfil a SAR or freedom of information (FOI) request. Emails will be drafted carefully, and staff members will review the content before sending.

11.7 Individuals, including children, have the right to submit an SAR to gain access to their personal data to verify the lawfulness of the processing – this includes accessing emails.

11.8 All SARs will be handled in accordance with the school's Data Protection Policy. FOI requests will be handled in accordance with the school's Freedom of Information Policy.

11.9 When handling a request for information, the DPO will speak to the requestor to clarify the scope of the request and whether emails will be required to fulfil the SAR or FOI request. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format. All requests will be responded to without delay and at the latest, within one month of receipt. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal. Staff members will discuss any queries regarding email retention with the DPO.

12.0 Storing and Protecting Information

12.1 The DPO will ensure a back-up of information takes place on a termly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

Where possible, backed-up information will be stored off the school premises, using a central back-up cloud service. The DPO will ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored on it.

12.2 Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access. Any room or area where personal or sensitive data is stored will be locked when unattended. Confidential paper records are not left unattended or in clear view when held in a location with general access.

12.3 Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site. Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

12.4 All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft. Staff and governors do not use their personal laptops or computers for school purposes. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

12.5 Emails containing sensitive or confidential information are password-protected or sent via a secure encrypted or data transfer system to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email. Personal information is never put in the subject line of an email. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

12.6 Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the UK GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

12.7 Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

12.8 The school has data sharing agreements with all data processors and third parties with whom data is shared. These agreements are developed by the DPO and cover information about issues such as access controls and permissions.

12.9 A record is kept of what level of access each staff member has to data. This record details information including:

- What level of access each staff member has.
- Limits on how staff members access data.
- What actions staff members can perform.
- What level of access is changed or retained when a staff member changes role within the school.
- Who is able to authorise requests to change permissions and access.

12.10 All staff members implement a ‘clear desk policy’ 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.

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

12.12 Staff are required to use their school login details to use photocopiers and printers.

12.13 The physical security of the school’s buildings and storage systems, and access to them, is reviewed termly by the site manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the headteacher and extra measures to secure data storage will be put in place.

12.14 All systems that allow staff and pupils to remotely access information from the school’s network whilst they are not physically at the school have strong security controls in place which are reviewed termly by the DPO. The DPO decides what restrictions are necessary to prevent information or records being downloaded, transferred or printed while the user is not on the school site.

12.15 The DPO is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data. Any damage to or theft of data will be managed in accordance with the school’s Data and Cyber-security Breach Prevention and Management Plan.

13.0 Accessing Information

13.1 We are transparent with data subjects about the information we hold and how it can be accessed.

13.2 All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the UK GDPR.

13.3 All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the UK GDPR, to access certain personal data being held about them or their child.

13.4 Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents. Pupils who are considered by the school to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

13.5 The school will adhere to the provisions outlined in the school’s Data Protection Policy when responding to requests seeking access to personal information.

14.0 Digital Continuity Statement

14.1 Digital data that is retained for longer than six years will be identified by the DPO and named as part of a Digital Continuity Statement. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with this policy.

14.2 Memory sticks are never used to store digital data, subject to a Digital Continuity Statement.

14.3 The ICT technician will review new and existing storage methods annually and, where appropriate, add them to the digital continuity statement.

14.4 The following information will be included within the Digital Continuity Statement:

- A statement of the business purposes and statutory requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the UK GDPR

15.0 Information Audit

15.1 The school conducts information audits on an annual basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the UK GDPR.

15.2 Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Data Asset Register. An information asset owner is assigned to each asset or group of assets. They will be responsible for managing the asset appropriately, ensuring it meets the school's requirements, and for monitoring risks and opportunities.

15.3 The information displayed on the Data Asset Register will be shared with the headteacher to gain their approval and sent to the Trust.

16.0 Disposal of Data

16.1 Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

16.2 All records containing personal or sensitive information will be made either unreadable or un-reconstructable.

16.3 Where disposal of information is outlined as secure disposal, this will be shredded or pulped. Electronic information will be scrubbed clean and, where possible, cut, archived or digitalised. The DPO will keep a record of all files that have been destroyed.

16.4 Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO

will keep a record of this. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

16.5 Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

16.6 Where information must be kept permanently, this information is exempt from the normal review procedures.