Data Protection Policy

ST CLARE
Catholic Multi Academy Trust

St Thomas of Canterbury School

To nurture curiosity for every child, everyday within a community acting as a beacon of the Catholic Faith.

Adopted by St Clare Trust Board; June 2022

Next review by St Clare Trust Board; June 2023

Reviewed by Local Academy Committee; December 2022

St Clare Catholic Multi Academy Trust Data Protection Policy

This policy should be read in conjunction with the following documents:

- Privacy Notice for Pupils
- Privacy Notice for the Trust Workforce
- Privacy Notice for Governors
- Privacy Notice for Job Applicants
- Privacy Notice – Common to All
- Privacy Notice for Trust/School Trips
- Privacy Notice for Payroll
- Images Policy for Pupils
- Images Policy for the Trust/School Workforce

St Clare Multi Academy Trust is registered with the Information Commissioner's Office. The registration number is ZB288989.

The Data Protection Officer (DPO) for the trust is Adnan Bashir. The DPO can be contacted by phone on 0114 256 6401 (Ask for St Clare Multi Academy Trust) or via the contact form on the trust website https://www.stclarecmat.org.uk/contact-us/

However, our data protection lead has day-to-day responsibility for data protection issues in our Trust/School. If you have any questions, concerns or would like more information about anything mentioned in this policy, please contact Sarah Hinchliffe, Office manager.

Roles and Responsibilities

Data Controller – determines the purposes and means of processing personal data. The Data Controller has an obligation to ensure that contracts with Data Processors comply with the General Data Protection Regulation.

Data Processor – responsible for processing personal data on behalf of a Data Controller. The Data Processor is required to maintain records of personal data and processing activities, and will have legal liability if the Data Processor is responsible for a breach.

General Data Protection Regulation (GDPR) May 2018

The GDPR is European-wide legislation is an update to the 1998 Data Protection Act. As a Public Organisation, the Trust/School has a statutory duty to adhere to the GDPR.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way we collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The GDPR refers to sensitive personal data, including genetic data, and biometric data where processed to uniquely identify an individual.

The principles of the GDPR state that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

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

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

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

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

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

With regards to e) above, although our privacy statements draw specific attention to the storage of particular types of personal data, unless stated otherwise in a privacy statement, the Trust/School will adhere to the Information Records Management Society Retention Schedule, which is included in Appendix A.

Data Protection Officer (DPO)

The CEO will appoint a Data Protection Officer. As per Article 39 of the GDPR, the DPO must:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff, and conduct internal audits;
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

The DPO keeps a record of those staff who have attended Data Protection training. The DPO reports to the CEO.

The DPO operates independently and will not be dismissed or penalised for carrying out the role. Adequate

resources are provided to enable the DPO to meet their GDPR obligations.

Privacy Notices

The Trust/School has a Privacy Notice for Pupils, and for the Trust Workforce, outlining:

- The legal basis on which we collect and process personal data, and what we use the data for;
- The categories of personal data that we collect and process;
- Details of who we share personal data with; The length of time that we retain personal data.

The Privacy Notice makes explicit an individual's rights under the GDPR.

The Privacy Notice provides contact details for all enquiries relating to Data Protection in the trust/school.

Any documentation where we collect personal data from individuals will contain a reference that

clearly signposts the Privacy Notice.

Sharing Personal Data

The Trust/School will share personal data with other Data Controllers where required to do so by law, only to the extent required by the relevant law. The Trust/School will only do so if there is a legal basis for the data sharing, and will include details of such data sharing in its Privacy Notices.

A Data Processor is an individual or organisation (a third party) who processes personal data on our behalf. Whenever a Data Controller uses a Data Processor, it needs to have a written contract in place, so that both parties understand their obligations, responsibilities and liabilities. The Trust/School will only appoint Data Processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects will be protected.

Where the data sharing is not undertaken on a statutory basis, (for example pupil images for Trust/School photographs, passport details with travel companies for students on a foreign Trust/School trip), we will ensure that we have either:

- a contractual agreement for the sharing of data with the company concerned demonstrating compliance to GDPR*, or;

- in those situations where pupils are using educational websites as part of their curriculum and we are not able to obtain a signed contract from the website concerned, we will require as a minimum a copy of an up-to-date privacy statement from the company that satisfactorily demonstrates their compliance to GDPR for the purposes of the data sharing concerned.

As a matter of good practice, our contracts:

- State that nothing within the contract relieves the Data Processor of its own direct responsibilities and liabilities under the GDPR; and
- Reflect any indemnity that has been agreed.

Data Breaches

The DPO will maintain a register of data breaches. The template for recording data breaches is provided in Appendix D.

Where a data breach is likely to result in a risk to the rights and freedoms of individuals (for example if unaddressed the breach is likely to result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage) the DPO will report the breach to the supervisory authority (currently the Information Commissioner's Office) within 72 hours of the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

Data Retention

The Trust/School will adhere to statutory guidance relating to the retention of personal data.

The Trust/School will adhere to the operational guidance provided by the Information Records Management Society.

The Trust/School's Data Retention Schedule is contained in Appendix A.

Data destruction involves the disposal of paper copies of the personal data, and deletion of electronic files from the Trust/School system. All staff will ensure that they are not retaining paper records or electronic files containing personal data for longer than the period indicated in the Trust/School's Data Retention Schedule.

The Trust/School keeps an electronic back up of the computer systems. Back-up data may be retained in a back-up format for a longer period than recommended by the Information Records Management Society. This is unavoidable, given the finite resources of the organisation.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment will be carried out whenever an individual or group of individuals within the organisation is considering a project that:

- Involves sharing personal data with a company or organisation that is not listed in a Privacy Notice, or for a purpose different to that stated in a Privacy Notice;
- Alters a Trust/School system in such a way as to involve a substantial change to the way in which personal data is processed.

This includes sharing data with companies that are not explicitly named in a Privacy Notice (e.g. a travel company who are providing a Trust/School trip).

The first stage of the Data Protection Impact Assessment is the project leader considering the questions

listed in Appendix E (DPIA Part 1).

If the answer to any of the questions in Appendix E is 'yes', the project leader will complete Appendix F (DPIA Part 2).

Management of the Trust/School

This section contains retention periods connected to the general management of the Trust/School. This covers the work of the Directors, Local Academy Committee, Trust Executive Team (e.g. CEO and CFO), the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Trust Board/Local Academy Committee							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
1.1.1	Agendas for Trust Board/Local Academy Committee meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]	Yes	CLK
1.1.2	Minutes of Trust Board/Local Academy Committee meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff				Yes	CLK
	Principal Set (signed)			PERMANENT	If the Trust/School is unable to store these then they should be offered to the County Archives Service		
	Inspection Copies[2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.		

[1] In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the Trust/School has the facility, shredding using a cross cut shredder.

[2] These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.1 Trust Board/Local Academy Committee							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
1.1.3	Reports presented to the Trust Board/Local Academy Committee	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes	Yes	CLK
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL	No	
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the Trust/School whilst the Trust/School is open and then offered to County Archives Service when the Trust/School closes.	No	
1.1.6	Trusts and Endowments managed by the Trust Board/Local Academy Committee	No		PERMANENT	These should be retained in the Trust/School whilst the Trust/School is open and then offered to County Archives Service when the Trust/School closes.	No	
1.1.7	Action plans created and administered by the Trust Board/Local Academy Committee	No		Life of the action plan + 3 years	SECURE DISPOSAL	No	
1.1.8	Policy documents created and administered by the Trust Board/Local Academy Committee	No		Life of the policy + 3 years	SECURE DISPOSAL	No	
1.1.9	Records relating to complaints dealt with by the Trust Board/Local Academy Committee	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL	Yes	CLK

1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL	No	
1.1.11	Proposals concerning the change of status of a maintained Trust/School including Specialist Status Trust/Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL	No	

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

1.2 CEO, CFO, Headteacher and School/Trust Senior Management Teams

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
1.2.1	Log books of activity in the Trust/School maintained by the CEO/Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate	Yes	PA
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL	Yes	PA
1.2.3	Reports created by the CEO/Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL	Yes	PA
1.2.4	Records created by CEO, CFO, head teachers, deputy head teachers, other executive staff or school leaders and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL	Yes	PA

1.2.5	Correspondence created by CEO, CFO, head teachers, deputy head teachers, other executive staff or school leaders and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL	Yes	PA
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL	Yes	PA
1.2.7	Trust/School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL	No	

1.3 Admissions Process							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
1.3.1	All records relating to the creation and implementation of the Trust/School Admissions' Policy	No	Trust/School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, Trust/Schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL	No	
1.3.2	Admissions – if the admission is successful	Yes	Trust/School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, Trust/Schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL	Yes	AM
1.3.3	Admissions – if the appeal is unsuccessful	Yes	Trust/School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, Trust/Schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL	Yes	AM
1.3.4	Register of Admissions	Yes	Trust/School attendance: Departmental advice for maintained Trust/Schools, academies, independent Trust/Schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	REVIEW Trust/Schools may wish to consider keeping the admission register permanently as often Trust/Schools receive enquiries from past pupils to confirm the dates they attended the Trust/School.	Yes	AM
1.3.5	Admissions – Secondary Trust/Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL	Yes	AM

1.3 Admissions Process							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	Trust/School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, Trust/Schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL	Yes	AM
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes				Yes	AM
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL		
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL		

1.4 Operational Administration							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL	No	
1.4.2	Records relating to the creation and publication of the Trust/School brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL	No	
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL	No	
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL	No	
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL	Yes	PA
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL	Yes	PA

This table has been taken from guidance published as the Information Management Toolkit for

Human Resources

This section deals with all matters of Human Resources management within the Trust/School.

2.1 Recruitment

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
2.1.1	All records leading up to the appointment of a new CEO or Head Teacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL	Yes	HR
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL	Yes	HR
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL	Yes	HR
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education)	The Trust/School does not have to keep copies of DBS certificates. If the Trust/School does so the copy must NOT be retained for more than 6 months		Yes	HR
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file		Yes	HR

2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years		Yes	HR

[4] Employers are required to take a "clear copy" of the documents which they are shown as part of this process.

2.2 Operational Staff Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL	Yes	HR
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL	Yes	HR
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL	Yes	HR

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data	Owner
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2022"; "Working together to safeguard children. A guide to interagency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded	Yes	HR
2.32	Disciplinary Proceedings	Yes			SECURE DISPOSAL These records must be shredded	Yes	HR
	Oral Warning			Date of warning[6] + 6 months			
	Written Warning – Level 1			Date of warning[6] + 6 months			
	Written Warning – Level 2			Date of warning[6] + 12 months			
	Final Warning			Date of warning[6] + 18 months			
	Case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL		

[5] This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.

[6] Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice.

1.4 Operational Administration							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL		
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL		
2.4.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL	Yes	HR
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980			Yes	HR
	Adults			Date of the incident + 6 years	SECURE DISPOSAL		
	Children			DOB of the child + 25 years	SECURE DISPOSAL		
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL	No	
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL	No	
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL	No	

2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL	No	

2.5 Payroll and Pensions							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL	Yes	HR
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL	Yes	HR

Financial Management of the Trust/School

This section deals with all aspects of the financial management of the Trust/School including the administration of Trust/School meals.

3.1 Risk Management and Insurance							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the Trust/School + 40 years	SECURE DISPOSAL	No	

3.2 Asset Management

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL	No	
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM

3.3 Accounts and Statements including Budget Management

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL	Yes	SBM/CFO
3.3.2	Loans and grants managed by the Trust/School	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL	Yes	SBM/CFO
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL	Yes	SBM/CFO
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL	Yes	SBM/CFO
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO

3.4 Contract Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL	Yes	SBM/CFO
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL	Yes	SBM/CFO

3.5 Trust/School Fund

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
3.5.1	Trust/School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL	No	
3.5.2	Trust/School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL	No	
3.5.3	Trust/School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.5.4	Trust/School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.5.5	Trust/School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.5.6	Trust/School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
3.5.7	Trust/School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO

3.6 Trust/School Meals Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
3.6.1	Free Trust/School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL	Yes	AM
3.6.2	Trust/School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL	Yes	AM
3.6.3	Trust/School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL	No	

Property Management

This section covers the management of buildings and property.

4.1 Property Management

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
4.1.1	Title deeds of properties belonging to the Trust/School	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry		No	
4.1.2	Plans of property belong to the Trust/School	No		These should be retained whilst the building belongs to the Trust/School and should be passed onto any new owners if the building is leased or sold.		No	
4.1.3	Leases of property leased by or to the Trust/School	No		Expiry of lease + 6 years	SECURE DISPOSAL	Yes	SBM/CFP
4.1.4	Records relating to the letting of Trust/School premises	No		Current financial year + 6 years	SECURE DISPOSAL	Yes	SBM

4.2 Maintenance

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
4.2.1	All records relating to the maintenance of the Trust/School carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
4.2.2	All records relating to the maintenance of the Trust/School carried out by Trust/School employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO

Pupil Management

This section includes all records which are created during the time a pupil spends at the Trust/School. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437			Yes	DSL
	Primary			Retain whilst the child remains at the primary Trust/School	The file should follow the pupil when he/she leaves the primary Trust/School. This will include: • to another primary Trust/School • to a secondary Trust/School • to a pupil referral unit • If the pupil dies whilst at primary Trust/School the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent Trust/School, transfers to home Trust/Schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Trust/Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority		
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL		
5.1.2	Examination Results – Pupil Copies	Yes				Yes	DSL
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.		

	Internal			This information should be added to the pupil file			

5.1 Pupil's Educational Record

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention							
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for Trust/Schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded	Yes	DSL
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for Trust/Schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review. This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded	Yes	DSL

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
5.2.1	Attendance Registers	Yes	Trust/School attendance: Departmental advice for maintained Trust/Schools, academies, independent Trust/Schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL	Yes	DSL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL	Yes	DSL

5.3 Special Educational Needs

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.	Yes	SENCO
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	Yes	SENCO

5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	Yes	SENCO
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold	Yes	SENCO

Curriculum Management

6.1 Statistics and Management Information							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
6.1.1	Curriculum Returns	No		Current year + 3 years	SECURE DISPOSAL	Yes	DM
6.1.2	Examination Results (School's Copy)	Yes		Current year + 6 years		Yes	AS
	SATS Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison			
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete			
6.1.3	Published Admission Number (PAN) Reports	No		Current year + 6 years		No	AM
6.1.4	Value Added and Contextual Data	No		Current year + 6 years		Yes	AS
6.1.5	Self-Evaluation Forms	No		Current year + 6 years		Yes	AS

S

6.2 Implementation of Curriculum							
Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL	No	
6.2.2	Timetable	No		Current year + 1 year		Yes	AS
6.2.3	Class Record Books	No		Current year + 1 year		Yes	AS
6.2.4	Mark Books	No		Current year + 1 year		Yes	AS
6.2.5	Record of homework set	No		Current year + 1 year		Yes	AS
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the Trust/School's policy then current year + 1 year	SECURE DISPOSAL	Yes	AS

Extra Curricular Activities

7.1 Educational Visits outside the Classroom							
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
7.1.1	Records created by Trust/Schools to obtain approval to run an Educational Visit outside the Classroom – Primary Trust/Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL	Yes	TVL
7.1.2	Records created by Trust/Schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Trust/Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL	Yes	TVL
7.1.3	Parental consent forms for Trust/School trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most Trust/Schools do not have the storage capacity to retain every single consent form issued by the Trust/School for this period of time.	Yes	TVL
7.1.4	Parental permission slips for Trust/School trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils		Yes	TVL

7.2 Walking Bus

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be suSBMitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]	Yes	N/A

7.3 Family Liaison Officers and Home Trust/School Liaison Assistants

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
7.3.1	Day Books	Yes		Current year + 2 years then review		Yes	DSL
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending Trust/School and then destroy		Yes	DSL
7.3.3	Referral forms	Yes		While the referral is current		Yes	DSL
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy		Yes	DSL
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy		Yes	DSL
7.3.6	Group Registers	Yes		Current year + 2 years		Yes	DSL

Central Government and Local Authority

This section covers records created in the course of interaction between the Trust/School and the local authority.

8.1 Local Authority							
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL	Yes	AM
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL	Yes	AM
8.1.3	Trust/School Census Returns	No		Current year + 5 years	SECURE DISPOSAL	Yes	AM
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL	Yes	AM

8.2 Central Government							
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record	Personal Data?	Owner
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL	Yes	PA
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL	Yes	SBM/CFO
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL	Yes	SBM/CFO

This section lists those personnel who have been assigned a role within this document.

Role	Name of Personnel	Location
Clerk (CLK)	Anna Poole	St Thomas of Canterbury School
PA to leadership team (PA)	Office Staff	St Thomas of Canterbury School
Administration Manager (AM)	Sarah Hinchcliffe	St Thomas of Canterbury School
School Business Manager (SBM)	Sarah Hinchcliffe	St Thomas of Canterbury School
CFO	Adnan Bashir	St Clare CMAT
HR Lead * (HR) *This may be the SBM in some settings	Sarah Hinchcliffe	St Thomas of Canterbury School
Designated Safeguarding Lead (DSL)	Louise Clements	St Thomas of Canterbury School
SENCO	Kate Heaton	St Thomas of Canterbury School
Trips and Visits Lead (TVL)	Louise Clements	St Thomas of Canterbury School
All Staff (AS)	All Staff	St Thomas of Canterbury School

Appendix C – Data Processor Minimum Contract Requirements

Our contracts include the following compulsory details:

1. The subject matter and duration of the processing;
2. The nature and purpose of the processing;
3. The type of personal data and categories of data subject; and
4. The obligations and rights of the Data Controller.

Our contracts include the following compulsory terms:

a. The Processor must only act on the written instructions of the Controller (unless required by law to act without such instructions);

b. The Processor must ensure that people processing the data are subject to a duty of confidence;

c. The Processor must take appropriate measures to ensure the security of processing;

d. The Processor must only engage a sub-processor with the prior consent of the Data Controller and a written contract;

e. The Processor must assist the Data Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

f. The Processor must assist the Data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

g. The Processor must delete or return all personal data to the Controller as requested at the end of the contract; and

h. The Processor must suSBMit to audits and inspections, provide the Controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

As a matter of good practice, our contracts:

i. State that nothing within the contract relieves the Processor of its own direct responsibilities and liabilities under the GDPR; and

ii. Reflect any indemnity that has been agreed.

Appendix D – Data Protection Breach Register

Details of the Data Protection Breach	
Date of incident:	
Please describe the incident in as much detail as possible.	
What measures did the Trust/School have in place to prevent an incident of this nature occurring?	
Please provide extracts of any policies & procedures the Trust/School has in place that you consider to be relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.	

Personal data placed at risk	
What personal data has been placed at risk?	
How many individuals were affected?	
Are the affected individuals aware that the incident has occurred?	
Has the data placed at risk now been recovered? If so please provide details of how and when.	
What steps has the Trust/School taken to prevent a recurrence of this incident?	

Training and Guidance
Does the Trust/School provide its staff with training on the requirements of Data Protection legislation? If so, please provide any extracts relevant to this incident.
Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

Does the Trust/School provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

Appendix D – Data Protection Breach Register

Previous contact with the Information Commissioner's Office (ICO)	
Have you reported any previous incidents to the ICO in the last two years?	
If the answer to the above question is yes, please provide brief details, including the date that it was reported and the ICO reference number.	

Miscellaneous	
Have you notified any other data protection authorities about this incident?	
If the answer to the above question is yes, please provide details.	
Have you informed the police about this incident?	
If the answer to the above question is yes, please provide details.	
Have you informed any other regulatory authorities about this incident?	
If the answer to the above question is yes, please provide details.	
Has there been any media coverage about this incident?	
If the answer to the above question is yes, please provide details.	

These questions will help you to decide whether a more detailed Data Protection Impact Assessment is necessary.

If the answer to any of the following questions is 'yes' then you **must** complete the Data Protection Impact Assessment Part 2 outlined in Appendix F, and lodge the completed Part 2 form with the Data Protection Officer.

Brief outline of the project	
Name of the person completing this form:	
Date:	

1. Will the project involve the collection of new personal data about individuals?

2. Will the project compel individuals to provide personal data about themselves?

3. Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the data? This includes different departments and other Trust/Schools (including Teaching Trust/Schools).

4. Will you be using personal data about individuals for a purpose it was not originally collected for?

5. Does the project involve you using new technology which might be perceived as being privacy intrusive?

6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

7. Is the personal data of a kind particularly likely to raise privacy concerns or expectations? For example employees' records or pupils' educational records.

8. Will the project require you to contact individuals in ways which they may find intrusive?

If you answered 'yes' to any of the questions in Appendix E, then you must complete the table below.

If you are unsure of the process, you must speak to the Data Protection Officer.

Step one: Identify the need for a DPIA
Explain what the project aims to achieve. What are the benefits to the Trust/School, to individuals and to other parties?
Summarise why the need for a DPIA was identified.

Step two: Describe the information flows
Summarise how personal data will be collected, used, stored, secured and deleted during the project.
Summarise which employees/departments/external organisations will have access to personal data during the project that would not usually be able to access the personal data.

Step three: Identify the privacy and related risks					
Identify the key privacy risks and the associated compliance and corporate risks.					
Privacy issue	**Risk to individuals / Compliance Risk[7]**	**Consultation / Actions to be taken**	**Detail Privacy Solutions identified**	**Evaluate Privacy Solutions** Is the final impact on individuals a justified, compliant and proportionate response to the aims of the project?	**Detail Approved Solution**

[7] The following are possible risks to individuals that should be considered:

- Information being shared inappropriately through inadequate disclosure controls.
- Information being used for a new purpose without the individual's knowledge.
- New surveillance methods creating an unjustified intrusion on privacy.
- Intrusive measures being taken against individuals as a result of collecting the information.
- The sharing or merging of data sets can allow organisations to collect a much wider set of information than individuals might expect.
- Enabling identifiers to be linked to anonymised data may mean it is no longer safely anonymised.

Step four: Integrate the DPIA outcomes into the project plan		
Detail who is responsible for integrating the DPIA outcomes back into the project plan.		
Action to be taken	**Responsibility**	**Date for completion**

Step eight: Post project review
Detail the results of the post project review.