Good Shepherd Trust
Life in all its fullness

DATA PROTECTION POLICY

The Good Shepherd Trust

Life in all its fullness

Version Number	Version Description	Date of Revision
1	Date of Adoption	January 2016
2	Reviewed	May 2018
3	Reviewed	September 2019
4	Reviewed	June 2020
5	Reviewed	May 2022
6	Reviewed	April 2024
7	Reviewed & Updated (legislation)	May 2026
8	Date of next review	May 2028

Data Protection Organisation Information

Data Protection Officer (DPO):	Jane Abington
DPO Contact Email:	dpo@thegoodshepherdmat.co.uk
ICO Registration Number:	ZA099650
Report a Data Breach:	By email: dpo@thegoodshepherdmat.co.uk
Report a SAR or FOI Request:	dpo@thegoodshepherdmat.co.uk
For help and guidance:	gov.uk: Data Protection in Schools | ico.org.uk | kymallanhub.co.uk

Contents

Data Protection Organisation Information 2
Contents 2
1. Values 4
2. Definitions and Terminology 4
Terminology within the Trust 5
Associated Policies and Documents 5
3. Introduction and Aims 6
Legislative Framework 6
Aims 6
The UK GDPR Data Protection Principles 7
4. The Data Controller and Designated Data Controllers 7
5. Data Protection Officer Role & Responsibilities 8
The Role of the DPO 8
6. Responsibilities of Staff 9
General Responsibilities 9
Responsibilities Regarding Own Data 9
7. Rights to Access Information (Subject Access Requests) 10

7.1 Receiving a Subject Access Request 10
7.2 Information an Individual Can Request 11
7.3 Clarifying a SAR 11
7.4 Encouraging Self-Service 11
7.5 Verifying Identity 11
7.6 Responses to a SAR 11
7.7 Accessing Pupils' Information 11
7.8 Timeframes for Responding to a SAR 12
8. Exempt Information 12
9. Dealing with Data Breaches 13
9.1 What is a Data Breach? 13
9.2 Breach Detection, Investigation, Reporting and Monitoring 13
9.3 Assessing the Risk 13
9.4 External Notification of Breaches 14
10. Data Protection Impact Assessments 14
10.1 Surveillance Cameras 15
11. Retention of Data 15
12. Data Retention Policy 15
12.1 Data Protection 16
12.2 Retention Schedule 16
12.3 Destruction of Records 21
12.4 Retention of Safeguarding Records 22
12.5 Archiving 22
12.6 Transferring Information to Other Media 22
12.7 Transferring Information to Another Trust (Primary Schools) 22
12.8 Emails 23
12.9 Responsibility and Monitoring 23
List of Appendices and Additional Documents 23
Appendices 23
Additional Documents 23

(Right-click the contents above and choose 'Update Field' in Word to populate page numbers.)

1. Values

In keeping with our Trust values, every member of the Trust family of schools will be valued and encouraged to fulfil their potential. In our Trust we believe:

- Everyone has something to offer
- Trust, honesty, empathy and social responsibility are the Christian values that frame our work
- We are here for the whole person, spiritually, morally, educationally and socially
- In working with transparency and openness

2. Definitions and Terminology

The proprietor is The Good Shepherd Trust Multi Academy Trust.

For the purposes of this Policy and procedures a child, young person, pupil or student is referred to as a 'child' or a 'pupil' and they are normally under 18 years of age.

'Parent' — wherever used, this includes any person with parental authority over the child concerned, e.g. carers, legal guardians.

'School' or 'setting' — wherever used, this refers to our central office and each of our academies and includes any wrap-around care provided and delivered by that setting, such as After School Clubs and Breakfast Clubs.

'Data processors' are third party organisations which process data on our behalf. They make no decisions about how and why they do that; they just do what we ask them to within the terms of our contract.

'Data subjects' are the people about whom we hold data. They fall into several categories: our workforce and their next of kin; pupils, their next of kin, and other professionals involved with them; contractors; and agency or partner organisation workers.

'Personal data' is any manually or digitally recorded information relating to a living person which identifies them, e.g. a name, email address, identification number, location data, image, IP address, or factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

'Sensitive personal data' or 'special category data' includes disability status, sexual orientation, sex life, ethnicity, medical information (physical and mental health), political, philosophical and religious opinions/beliefs, trade union

membership, and details of criminal convictions or allegations. This category requires enhanced security measures.

'Pseudonymised personal data' is information that has been de-personalised but key-coded. It can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

'Supervisory Authority' is the body that regulates compliance with the UK GDPR. In the UK this is the Information Commissioner's Office (ICO).

'Third country' is a country where there is no privacy and data security equivalence agreement, and transfers of personal data are restricted unless specially protected or an exception applies.

Terminology within the Trust

Role/Term	Alternatives, Description and Meaning
Members	Members appoint the Directors. Membership is described in the Trust's Articles of Association.
Trustees	Also 'the Trust board' or 'the board'. The Trustees are accountable in law for all decisions about member schools and are accountable to the Secretary of State for Education for the performance of each school within the Trust.
LGB	Also 'Local Governing Bodies' or 'LGB Members'. The local governing body is a standing committee of the Trust which has delegated powers to oversee the running of its individual school. The LGB may choose to delegate some of these powers to smaller committees or the Headteacher as it deems fit to fulfil its responsibilities.
CEO	Chief Executive Officer. A significant number of responsibilities under the scheme of delegation lie with the CEO, who may delegate some duties to other staff.
Central Hub	Refers collectively to the Deputy CEO, Head of Finance, People Partner, Governance and Compliance Lead and any other appropriate staff based at the Trust's central administration office.
SLT	Senior Leadership Team: The Headteacher/Executive Headteacher, Head of School, Deputy Headteacher or other Senior staff member as appropriate. 'Headteacher' in policies will usually refer to the Headteacher or Executive Headteacher as appropriate.

Associated Policies and Documents

- Overarching Safeguarding Statement
- Child Protection Policy and procedures
- Online Safety Policy and procedures
- Freedom of Information Publication Scheme

- Health and Safety Policy and procedures
- Procedures for Using Pupils' Images
- Behaviour Policy and procedures
- Staff Code of Conduct
- Surveillance Camera Procedures (where applicable)

3. Introduction and Aims

This is a Trust-wide policy designed to cover all our schools and central operations. It is a statement of the aims and principles of the whole Trust for ensuring the appropriate handling of personal and sensitive information. This policy takes due note of the information and guidance published by the Information Commissioner's Office (ICO).

It is the responsibility of the Trust's Board of Directors to ensure registration with the ICO is undertaken and maintained.

Legislative Framework

The Trust's data protection practices are governed by the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005
- Children and Families Act 2014
- Special Educational Needs and Disability Act 2001
- Limitation Act 1980
- ICO guidance: Data Protection in Schools
- Department for Education (DfE) guidance on data protection

The Trust also has regard to the ICO's Children's Code (Age Appropriate Design Code), which sets out standards for online services likely to be accessed by children. Although primarily aimed at app and website providers, the principles inform how the Trust processes children's data in digital environments.

Aims

This policy sets out how the Trust's family of schools will:

- Comply fully with the requirements of the Data Protection Act 2018 and UK GDPR
- Ensure that all processing is appropriately registered / notified and review and update notified entries
- Ensure that all staff involved with the collection, processing and disclosure of personal data are made aware of their duties and responsibilities
- Demonstrate compliance with the Data Protection (DP) principles including implementing appropriate technical and organisational measures, maintaining records on processing activities, conducting data protection impact assessments, and undertaking data protection by design and default

The UK GDPR Data Protection Principles

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data

The Trust is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents, LGB members, directors, volunteers and any other individual whose personal data it holds.

4. The Data Controller and Designated Data Controllers

The Good Shepherd Multi Academy Trust as the corporate body is the Data Controller under the 2018 Act and UK GDPR. The Trust Board is ultimately responsible for implementation. The CEO (assuming they are also a Trustee) acts as the Designated Data Controller for the Trust as a whole.

Day-to-day responsibility for activity in each location is given to two Designated Data Controllers: the headteacher and the senior member of the office staff in each school, and the CEO and a named member of staff in the central office. They are responsible for ensuring that all staff and volunteers in their setting are

adequately trained and understand their responsibilities regarding data protection, including recognising a Subject Access Request and what to do once received.

The Trust's central hub will coordinate a data audit and produce and manage a central data register. It is the responsibility of each location's Designated Data Controllers to review the register on a regular basis and report any changes, including third parties with whom they share data.

Where individual locations enter into agreements with suppliers involving third-party data sharing, the Designated Data Controllers for that location must ensure that data sharing agreements are in place before proceeding and that the central data register is updated accordingly.

5. Data Protection Officer Role & Responsibilities

The Trust will appoint and support the Data Protection Officer (DPO) to take responsibility for data protection compliance and ensure they have the knowledge, support and authority to carry out their role effectively. The DPO can be contacted by emailing dpo@thegoodshepherdmat.co.uk.

The Trust has an appointed DPO because:

- Under the Data Protection Regulations, the processing carried out is to achieve a public task, e.g. education
- Core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale (FSM, grades, IHCPs/EHCPs)
- Core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences

The Role of the DPO

The DPO is responsible for:

- Taking responsibility for and monitoring data protection compliance
- Being the point of contact with the ICO (and for data subjects and workers within the Trust)
- Leading/advising on (not necessarily carrying out) DPIAs
- Taking a risk-based approach
- Maintaining data protection records

In delivering the DPO role, monitoring tasks will include:

- Collecting information to identify processing activities
- Analysing and checking compliance of processing activities
- Informing, advising and issuing recommendations to the controller/processor

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about themselves, or their child should raise the matter with the appropriate Designated Data Controller or the Data Protection Officer.

6. Responsibilities of Staff

All staff who process or use personal information must ensure they always follow the data protection principles. This policy does not form part of the contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the Trust's Board of Directors. Failures to follow the policy can result in disciplinary proceedings.

General Responsibilities

All staff are responsible for ensuring that:

- Any personal data they hold is kept securely
- All personal data is kept in a locked filing cabinet, drawer or safe; or if computerised, is encrypted or password-protected on a local hard drive and on a network drive that is regularly backed up
- Personal data is not downloaded or kept on a USB memory key or other removable storage media
- Personal information is not disclosed, orally or in writing, via web pages or by any other means, accidentally or otherwise, to any unauthorised third party
- All data breaches are reported using the process described in Section 9 of this policy
- All personal data is handled with reference to this policy and the Trust's Online Safety Policy
- They are fully aware of their responsibilities regarding data protection including attending awareness-raising sessions and workshops as required

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Responsibilities Regarding Own Data

Regarding their own data, all staff are responsible for:

- Checking that any information they provide to the Trust in connection with their employment is accurate and up to date
- Informing the Trust of any changes to information provided, e.g. change of address. The Trust cannot be held responsible for errors unless the staff member has informed it of such changes

7. Rights to Access Information (Subject Access Requests)

All staff, parents and other individuals are entitled to know what information the Trust and its schools hold and process about them or their child and why; to gain access to it; to keep it up to date; and to know what the Trust is doing to comply with its obligations.

The Trust has produced four types of privacy notice (Appendix A):

- Privacy Notice – Workforce
- Privacy Notice – Governance Roles
- Privacy Notice – Pupils and Families
- Privacy Notice – Primary School Pupils (can be adapted with the school logo and name)

The Trust recognises that whilst parents/carers/legal guardians have the legal responsibility for and can agree to the use of their child's personal data for children younger than 13, it is good practice to engage with and aid the understanding of those pupils. The primary school pupils privacy notice has been designed to be relevant to and understood by younger pupils.

7.1 Receiving a Subject Access Request

Under Article 15 of the UK GDPR all individuals have a right to access certain personal data kept about them or their child either digitally or in hard copy. Any person who wishes to exercise this right should make a request in writing and submit it to:

Email: dpo@thegoodshepherdmat.co.uk

Post: Data Protection Officer, 19-24 Friargate, Penrith, Cumbria, CA11 7XR

A SAR form is available (Appendix B) to help people complete their request; however, there is no requirement to use this form and a SAR can be made in any format including verbally, by letter, text, email or social media.

A request can be made to anyone who works at one of our settings, including teachers, support staff, volunteers and Local Governing Body members. The

Designated Data Controllers must ensure that everyone in their setting can recognise a SAR when it is made.

7.2 Information an Individual Can Request

A requestor can ask for personal data that relates to themselves; someone they have parental responsibility for; or someone they have permission to act on behalf of.

7.3 Clarifying a SAR

Some requests will be non-specific and ask for 'all the information held'. While we cannot ask the requestor to narrow their request, it is possible to seek clarification of what specific information is being sought.

7.4 Encouraging Self-Service

If the requestor already has access to the information they want (e.g. via Class Dojo or a similar platform), direct them to this. Where the requestor can access the information themselves within one calendar month, the request does not have to be treated as a SAR.

7.5 Verifying Identity

In most cases identity verification will be required. If the Data Controller knows the requestor and is sure of their identity, an ID request does not have to be completed, but a record of this decision must be kept.

Adults should provide photo ID (driving licence or passport) plus another form of ID such as a utility bill or council tax bill. Where requests are made on behalf of others, the authorisation and right of the third party to access the individual's data must be established before the request is dealt with.

7.6 Responses to a SAR

In fulfilling the SAR, a statement regarding the personal data held about the requestor will be provided. If no personal data is held, a response will still be made confirming this and, where relevant, why data is no longer held. There may be grounds for refusing or redacting information — see Section 8 and Appendix C.

7.7 Accessing Pupils' Information

7.7.1 Access under UK GDPR

The right to access information held about a child (Article 15, UK GDPR) is the child's right rather than anyone else's. Parents are only entitled to access information about their child if the child is unable to act on their own behalf or has

given their consent. Before responding to a SAR for information about a child, the setting's data controller will consider whether the child is mature enough to understand their rights.

7.7.2 Access under Education Regulations

Those with parental authority can request to view a child's education record under The Education (Pupil Information) (England) Regulations 2005. This right does not extend to pupils. The setting must comply with a written request within 15 school days (excluding school holidays). Those with parental authority must be given access to view the record free of charge. A fee may be charged for copies, not exceeding the cost of supply.

7.8 Timeframes for Responding to a SAR

A full SAR response must be sent to the requestor within one calendar month from the day the SAR is submitted. This timeframe cannot be extended due to school holidays. If the deadline will not be met, the requestor must be informed as soon as possible.

The deadline may be extended if waiting for the requestor to provide identification or clarification. If the request is complex, the response time can be extended by up to two further calendar months (three months total). If treated as complex, the requestor must be notified in writing within one calendar month of the original request date.

8. Exempt Information

The Data Protection Act 2018 allows exemptions as to the provision of some information. All information will be reviewed prior to disclosure. Refer to ICO guidance for further details.

Third-party information provided by another employee, child, parent, police, local authority, healthcare professional or another school will require their consent before it can be disclosed. Information which may cause serious harm to the physical, mental or emotional wellbeing of the pupil or any other person should not be disclosed, nor should information that would reveal a child is at risk of abuse or information relating to court proceedings.

Where redaction has taken place, a full copy of the information provided must be retained to establish, if a complaint is made, what was redacted and why. Guidance on how to respond when refusing a request for personal information is available in Appendix C.

9. Dealing with Data Breaches

9.1 What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes and is about more than just losing personal data.

Personal data breaches can include, but are not limited to:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

9.2 Breach Detection, Investigation, Reporting and Monitoring

When a security incident takes place, Trust staff will work quickly to establish whether a personal data breach has occurred, and prompt steps will be taken to address and contain it.

Every member of staff dealing with personal data has a responsibility to report a data breach that they are either responsible for or become aware of to their setting's Data Controller as soon as possible. Any qualifying breach must be reported to the ICO within 72 hours.

A record of all breaches will be kept (Appendix D), documenting the facts relating to the breach, its effects, the remedial action taken, the justification for reporting to the ICO or not, the justification for notifying individuals or not, the findings of any follow-up investigation, and recommendations to prevent recurrence.

9.3 Assessing the Risk

Before deciding on steps required beyond immediate containment, an assessment of the risks associated with the breach must be undertaken, including potential adverse consequences for individuals, how serious or substantial these are, and how likely they are to happen.

In assessing the risk, the following are considered:

- What type of data is involved and how sensitive is it?

- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- What could the data tell a third party about the individual?
- How many individuals are affected?
- What harm can come to those individuals?
- Are there wider consequences such as loss of public confidence in the Trust?

9.4 External Notification of Breaches

9.4.1 Notification of Individuals

Where a breach is likely to result in a 'high risk' to the rights and freedoms of individuals, Trust staff must inform those concerned directly and without undue delay. Where possible, specific guidance and clear advice will be given to affected individuals on steps they can take to protect themselves.

9.4.2 Notification of the Information Commissioner's Office

When a personal data breach with risk to people's rights and freedoms is identified, it must, where feasible, be reported to the ICO within 72 hours of identification.

ICO Reporting Helpline: 0303 123 113

Online reporting: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/

The external notification to the ICO should include a description of the nature of the breach; when it occurred; details of the risk assessment; measures taken or proposed; the likely consequences; and contact details of the DPO.

10. Data Protection Impact Assessments

The Good Shepherd Trust has a legal obligation to undertake Data Protection Impact Assessments (DPIAs) before carrying out any processing which is 'likely to result in high risk' to individuals' interests. This is a key element of data protection by design and default.

A DPIA must:

- Describe the processing and the purpose for data processing
- Assess necessity and proportionality
- Identify and assess risks to individuals

- Identify measures to mitigate those risks and protect the data

In particular, the Trust must carry out a DPIA where plans involve:

- Systematic and extensive profiling with significant effects
- Processing special category or criminal offence data on a large scale
- Systematically monitoring publicly accessible places on a large scale
- Use of new technologies
- Profiling or special category data to decide on access to services
- Processing biometric or genetic data
- Matching data or combining datasets from different sources
- Tracking individuals' location or behaviour
- Profiling children or targeting services at them

A DPIA should begin early in the life of a project and run alongside the planning and development process. It is not a one-off exercise and should be seen as an ongoing process. The advice of the Trust DPO must be sought in undertaking a DPIA. If a DPIA identifies a high residual risk that cannot be mitigated, the ICO must be consulted before the project starts.

10.1 Surveillance Cameras

When involving surveillance cameras, the government guidance template — Data Protection Impact Assessments for Surveillance Cameras (Additional Document F) — will be used. Kym Allan Health and Safety Consultants also provide model procedures for surveillance cameras if required.

11. Retention of Data

The Trust's Data Retention Policy (Section 12) provides detailed guidance and information on how, when and why data is retained and disposed of. This is based on advice from the Information Records Management Society Toolkit for Schools.

Personal data may only be kept for as long as it is needed. How long this is will depend on the circumstances and the reasons it was obtained. Different categories of data will be retained for different periods of time as set out in the Retention Schedule in Section 12.

12. Data Retention Policy

The Good Shepherd Trust has a responsibility to maintain its records and record keeping systems. When doing this, the Trust will take account of the following factors:

- The most efficient and effective way of storing records and information
- The confidential nature of the records and information stored
- The security of the record systems used
- Privacy and disclosure
- Accessibility of records and record keeping systems

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It may be amended by the Trust from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect.

12.1 Data Protection

This section sets out how long employment-related and pupil data will normally be held by the Good Shepherd Trust and when that information will be confidentially destroyed, in compliance with the terms of the UK GDPR and the Freedom of Information Act 2000.

12.2 Retention Schedule

Information (hard copy and electronic) will be retained for at least the period specified in the retention schedule below. The retention schedule refers to all records regardless of the media (e.g. paper, electronic, microfilm, photographic) in which they are stored. All records will be regularly monitored by internal reviews.

File Description	Retention Period
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the Trust has applicants' consent to keep their CVs for future reference
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	6 years after employment ceases

Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded. In exceptional circumstances, no longer than 6 months
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel records	While employment continues and up to 6 years after employment ceases (Limitation Act 1980)
Annual leave records	6 years after the end of the tax year to which they relate, or longer if leave can be carried over
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations – opt-out forms	Two years from the date on which they were entered into
Working Time Regulations – records of compliance	Two years after the relevant period
Disciplinary records	6 years after employment ceases
Training records	6 years after employment ceases or as required by the professional body
Staff training relating to safeguarding or child-related training	Date of training plus 40 years (reflects potential IICSA investigations)
Annual appraisal/assessment records	Current year plus 6 years
Professional Development Plans	6 years from the life of the plan
Allegations of a child protection nature against a member of staff (including founded allegations)	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). Malicious allegations should be removed.
Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to

Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	Until updated plus 3 years
Bonus Sheets	Current year plus 3 years
Time sheets / clock cards / flexitime	Current year plus 3 years
Pupil Premium Fund records	Date pupil leaves the Trust plus 6 years
National Insurance (schedule of payments)	Current year plus 6 years
Insurance	Current year plus 6 years
Overtime	Current year plus 3 years
Annual accounts	Current year plus 6 years
Loans and grants managed by the Trust	Date of last payment plus 12 years
All records relating to the creation and management of budgets	Life of the budget plus 3 years
Invoices, receipts, order books, requisitions and delivery notices	Current financial year plus 6 years
Student grant applications	Current year plus 3 years
Trust fund documentation (invoices, cheque books, receipts, bank statements etc.)	Current year plus 6 years
Free Trust meals registers (where used as a basis for funding)	Current year plus 6 years
Trust meal registers and summary sheets	Current year plus 3 years
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
Trust Development Plans	3 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Newsletters and circulars to staff, parents and pupils	1 year (the Trust may decide to archive one copy)
Minutes of Senior Management Team meetings	Date of meeting plus 3 years or as required
Reports created by the Head Teacher or Senior Management Team	Date of report plus a minimum of 3 years or as required
Records relating to the creation and publication of the Trust prospectus	Current academic year plus 3 years
Health and Safety Records	

Health and Safety consultations	Permanently
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years
Health and Safety Policy Statements	Life of policy plus 3 years
Any records relating to a reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years (all records to be held on personnel file)
Accident reporting records relating to individuals under 18 at the time of the incident	Until the child reaches the age of 21
Accident reporting records relating to individuals over 18 at the time of the incident	3 years after the last entry in the accident book
Fire precaution logbooks	Current year plus 3 years
Medical records and details: control of lead at work, asbestos dust, COSHH records	40 years from the date of the last entry
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Governing Body Documents	
Instruments of government	For the life of the Trust
Meetings schedule	Current year
Minutes – principal set (signed)	Generally kept for the life of the organisation
Agendas – principal copy	Should be stored with the principal set of minutes where possible
Agendas – additional copies	Date of meeting
Policy documents created and administered by the governing body	Until replaced
Register of attendance at full governing board meetings	Date of last meeting in the book plus 6 years
Annual reports required by the Department of Education	Date of report plus 10 years
Records relating to complaints made to and investigated by the governing body or headteacher	Major complaints: current year plus 6 years. If negligence involved: current year plus 15 years. If child protection or safeguarding issues involved: current year plus 40 years.
Correspondence sent and received by the governing body or headteacher	General correspondence: current year plus 3 years

Records relating to terms of office of serving governors, including evidence of appointment	Date appointment ceases plus 6 years
Register of business interests	Date appointment ceases plus 6 years
Records relating to training required and received by governors	Date appointment ceases plus 6 years
Records relating to the appointment of a clerk to the governing body	Date on which clerk appointment ceases plus 6 years
Governor personnel files	Date appointment ceases plus 6 years
Pupil Records	
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission
Proof of address supplied by parents as part of the admissions process	Current year plus 1 year
Admissions register	Entries to be preserved for 3 years from date of entry
Pupil Record	Primary – whilst the child attends the Trust. Secondary – until the child reaches the age of 25 (Limitation Act 1980)
Attendance Registers	3 years from the date of entry
Correspondence relating to any absence (authorised or unauthorised)	Current academic year plus 2 years
Special Educational Needs files, reviews and EHCPs, including advice and information to parents regarding educational needs and accessibility strategy	Date of birth of the pupil plus 31 years (EHCP valid until age 25, plus 6 years). See Children and Families Act 2014; Special Educational Needs and Disability Act 2001.
Child protection information (held in a separate file)	DOB of the child plus 25 years then review. Note: records will be subject to any IICSA instruction.
Exam results (pupil copy)	1–3 years from the date the results are released
Examination results (Trust's copy)	Current year plus 6 years
Allegations of sexual abuse	For the time period of an inquiry by the Independent Inquiry into Child Sexual Abuse
Records relating to any allegation of a child protection nature against a member of staff	Until the accused's normal retirement age or 10 years from the date of the allegation (whichever is the longer)
Consents relating to Trust activities under UK GDPR	Whilst the pupil attends the Trust

Pupil's work	Returned to pupil at the end of the academic year where possible; otherwise current year plus 1 year
Mark books	Current year plus 1 year
Schemes of work	Current year plus 1 year
Timetable	Current year plus 1 year
Class record books	Current year plus 1 year
Record of homework set	Current year plus 1 year
Photographs of pupils	For the time the child is at the Trust and for a short while after. Selected images may also be kept longer to illustrate the history of the Trust.
Parental consent forms for Trust trips (no major incident)	End of trip or end of academic year (subject to risk assessment)
Parental permission slips for Trust trips (major incident)	Date of birth of the pupil involved plus 25 years. Permission slips for all pupils on the trip should be retained.
Other Records	
Emails	Five years (NB: retention period depends on content; staff should file emails under the relevant category)
CCTV	One calendar month
Privacy notices	Until replaced plus 6 years
Inventories of furniture and equipment	Current year plus 6 years
All records relating to the maintenance of the Trust carried out by contractors or employees	Whilst the building belongs to the Trust
Records relating to the letting of Trust premises	Current financial year plus 6 years
Records relating to the creation and management of Parent Teacher Associations / Old Pupils Associations	Current year plus 6 years then review
Referral forms	While the referral is current
Contact data sheets	Current year then review; if contact is no longer active, destroy

12.3 Destruction of Records

Where records have been identified for destruction, they should be disposed of in an appropriate way. All information must be reviewed before destruction to

determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information or sensitive policy information should be shredded before disposal. All other paper records should be disposed of by an appropriate wastepaper merchant. All electronic information will be securely deleted.

The Trust maintains a database of records that have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record: file reference; file title/description; number of files; name of the authorising officer; date destroyed or deleted; and person(s) who undertook destruction.

12.4 Retention of Safeguarding Records

Any allegations found to be malicious must not be part of the personnel records.

For any other allegations, the Trust must keep a comprehensive summary of the allegation, details of how it was investigated and resolved, and any decisions reached. This should be kept on the personnel files of the accused.

Allegations of sexual abuse should be preserved for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse (IICSA). All other records should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer.

Whilst the IICSA is ongoing, it is an offence to destroy any records relating to it.

12.5 Archiving

Where records have been identified as worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of records sent to the archives is maintained by the Operations Manager. The appropriate staff member should record: file reference; file title/description; number of files; and name of the authorising officer.

12.6 Transferring Information to Other Media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to digital media or virtual storage (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

12.7 Transferring Information to Another Trust (Primary Schools)

We retain the pupil's educational record whilst the child remains at the Trust. Once a pupil leaves, the file should be sent to their next Trust and the responsibility for retention shifts accordingly. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

12.8 Emails

Email accounts are not a case management tool in themselves. The retention period for emails depends on their content — an email regarding a health and safety report will be subject to a different timeframe to an email forming part of a pupil record. It is important that staff file emails in the relevant areas to avoid data being lost.

12.9 Responsibility and Monitoring

The Operations Manager has primary day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the Trust, is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records. Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

List of Appendices and Additional Documents

Appendices

- Appendix A1: Privacy Notice – Workforce
- Appendix A2: Privacy Notice – Governance Roles
- Appendix A3: Privacy Notice – Pupils and Families
- Appendix A4: Privacy Notice – Pupils (Primary)
- Appendix B: SAR Form
- Appendix C: Refusing a Request for Personal Data
- Appendix D: Data Breach Log
- Appendix E: Data Protection Impact Assessment Template

Additional Documents

- Additional Document F: ICO DPIA for Surveillance Cameras

- KAHSC Model Surveillance Camera Procedures

All appendices are available on the members' area of the Trust website. Additional documents are available from the ICO and Kym Allan Health and Safety Consultants. The Pupils and Families Privacy Notice is available from all Trust websites. The Workforce Privacy Notice is available from the Trust's website and via the Trust's payroll app and portal.