

Data Retention Policy



Policy

Reviewed: March 2023
To be reviewed: March 2026

St. John's C.E. (C) Primary School

Data Retention Policy as part of Data Protection

Rationale

In keeping with the Christian ethos of St. John's C.E. (C) Primary School we are committed to maintaining the confidentiality of its information and ensuring that all records within the School are only accessible by the appropriate individuals. In line with the requirements of the Data Protection Act (2018) and General Data Protection Regulation (2018), the School also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The School has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the School's statutory requirements. This policy should be read in conjunction with the statutory Data Protection Policy.

Legal framework

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

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

Responsibilities

The School as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

The Governing Body holds overall responsibility for this policy and for ensuring it is implemented correctly.

The Head Teacher is responsible for the management of records in school along with the Data Protection Officer (DPO) Tim Pinto of The e-Safety Office.

The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the Head Teacher.

The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy and are disposed of correctly.

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

Management of pupil records

Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each School that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement. These records are maintained electronically using RM Integrus G2 Management Information System.

The following information is stored in a pupil record, and is only accessible by authorised personnel who have a valid username and password:

- Forename, surname, gender and date of birth
- Unique pupil number
- Note of the date when the file was opened
- Note of the date when the file was closed, if appropriate
- Ethnic origin, religion and first language (if not English)
- Any preferred names
- Position in their family, e.g. eldest sibling
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of parents, including their home address(es) and telephone number(s)
- Name of the School, admission number, the date of admission and the date of leaving, where appropriate
- Any other agency involvement, e.g. speech and language therapist
- Details of any SEND
- If the pupil has attended an early years' setting, the name of that setting and the child's attendance percentage
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Absence notes
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.

- Correspondence with parents about minor issues, e.g. behaviour

Hard copies of disclosures and reports relating to child protection are stored on CPOMS Management Information System and is only accessible by the Safeguarding Team who own a Merilock Key.

Hard copies of complaints made by parents or pupils are stored in a file in the Head Teacher's office.

Actual copies of accident and incident information are stored separately on the Kirklees Health and Safety LACHs Management Information System and held in line with the retention periods outlined in this

The School will ensure that no pupil records are altered or amended before transferring them to the next School that the pupil will attend.

The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed.

Electronic records relating to a pupil's record will also be transferred to the pupils' next School. [Section 10](#) of this policy outlines how electronic records will be transferred.

The School will not keep any copies of information stored within a pupil's record, beyond the outlined retention period, unless there is ongoing legal action at the time during which the pupil leaves the School. The responsibility for these records will then transfer to the next School that the pupil attends.

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

Retention of pupil records and other pupil-related information

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

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

Type of file	Retention period	Action taken after retention period ends
Admissions		
Register of admissions	Until the child's 25 th birthday	Information is reviewed and the register may be kept permanently
Proof of address (supplied as part of the admissions process)	Until the child's 25 th birthday	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Until the child's 25 th birthday	Securely disposed of
Pupils' educational records		
<u>Primary</u> Pupils' educational records	Until the child's 25 th birthday	Transferred to the next destination – if this is an independent School, home-Schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period
Internal examination results	Until the child's 25 th birthday	Securely disposed of
Child protection records held in a separate file	Until the child's 25 th birthday	Transferred to the next destination school
Attendance		
Attendance registers	Until the child's 25 th birthday	Securely disposed of
Letters authorising absence	Until the child's 25 th birthday	Securely disposed of

SEND		
SEND files, reviews and individual education plans	Until the child's 25 th birthday	Information is reviewed and the file may be kept for longer than necessary if it is required for the School to defend themselves in a 'failure to provide sufficient education' case
Statement of SEN maintained under section 324 of the Education Act 1996 or an EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	Until the child's 25 th birthday	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	Until the child's 25 th birthday	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	Until the child's 25 th birthday	Securely disposed of, unless it is subject to a legal hold
Curriculum management		
SATs results	Until the child's 25 th birthday	Securely disposed of
Examination papers	Until the appeals/validation process has been completed	Securely disposed of
Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms	Current academic year, plus six years	Securely disposed of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of

Extra-curricular activities		
Parental consent forms for School trips where no major incident occurred	Until the child's 25 th birthday	Securely disposed of
Parental consent forms for School trips where a major incident occurred	Until the child's 25 th birthday	Securely disposed of

Retention of staff records

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

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

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personnel file	Termination of employment, plus six years	Securely disposed of
Timesheets	Termination of employment, plus six years	Securely disposed of
Annual appraisal and assessment records	Termination of employment, plus six years	Securely disposed of
Recruitment		
Records relating to the appointment of a new Head Teacher	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Termination of employment, plus six years	Securely disposed of

DBS clearance	Termination of employment, plus 6 months	Securely disposed of
Proof of identify as part of the enhanced DBS check	Termination of employment, plus 6 years	Securely disposed of
Evidence of right to work in the UK	Termination of employment, plus 6 years	Securely disposed of

Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	<p>Added to staff personnel file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer</p> <p>If allegations are proved to be malicious, they are removed from personnel files</p>	Reviewed and securely disposed of
Oral warnings	Termination of employment, plus 6 years	Securely disposed of
Written warning – level 1	Termination of employment, plus 6 years	Securely disposed of
Written warning – level 2	Termination of employment, plus 6 years	Securely disposed of
Final warning	Termination of employment, plus 6 years	Securely disposed of

Records relating to unproven incidents	Termination of employment, plus 6 years	Securely disposed of
--	---	----------------------

Retention of senior leadership and management records

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

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

Type of file	Retention period	Action taken after retention period ends
Governing board		
Agendas for governing board meetings	Six years	Securely disposed of
Original, signed copies of the minutes of governing board meetings	Six years	If unable to store, these will be provided to the <u>local authority archive service</u>
Inspection copies of the minutes of governing board meetings	Six years	Securely disposed of
Reports presented to the governing board	Six years	Securely disposed of
Meeting papers relating to the annual parents' meeting	Six years	Securely disposed of
Instruments of government, including articles of association	Six years	If unable to store, these will be provided to the <u>local authority archives service</u>
Schools and endowments managed by the governing board	Six years	Retained in the School whilst it remains open, then provided to the <u>local authority archives service</u> when the School closes
Action plans created and administered by the governing board	Six years	Securely disposed of

Policy documents created and administered by the governing board	Six years	Securely disposed of
Records relating to complaints dealt with by the governing board	Six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Six years	Securely disposed of
Proposals concerning changing the status of the School	Six years	Securely disposed of
Head Teacher and senior leadership team (SLT)		
Log books of activity in the School maintained by the Head Teacher	Six years	Reviewed and offered to the local authority archives service if appropriate
Minutes of SLT meetings and the meetings of other internal administrative bodies	Six years	Securely disposed of
Reports created by the Head Teacher or SLT	Six years	Securely disposed of
Records created by the Head Teacher, Deputy Head Teacher other members of staff with administrative responsibilities	Six years	Securely disposed of
Correspondence created by the Head Teacher, Deputy Head Teacher and other members of staff with administrative responsibilities	Six years	Securely disposed of
Professional development plan	Six years	Securely disposed of
School development plan	Six years	Securely disposed of

Retention of health and safety records

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

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

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety policy statements	Six years	Securely disposed of
Health and safety risk assessments	Six years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Six years	Securely disposed of
Accident reporting – pupils	Child's 25 th birthday	Securely disposed of
Control of substances hazardous to health	40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	50 years	Securely disposed of
Fire precautions log books	Six years	Securely disposed of

Retention of financial records

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

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

Type of file	Retention period	Action taken after retention period ends
Payroll pensions		
Maternity pay records	Termination of employment, plus 6 years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Termination of employment, plus 6 years	Securely disposed of
Risk management and insurance		
Employer's liability insurance certificate	40 years – retained by Kirklees	Securely disposed of
Asset management		
Inventories of furniture and equipment	Six years	Securely disposed of
Burglary, theft and vandalism report forms	Six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Six years	Securely disposed of
Loans and grants managed by the School	Six years	Securely disposed of
All records relating to the creation and management of budgets	Six years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Six years	Securely disposed of
Records relating to the collection and banking of monies	Six years	Securely disposed of
Records relating to the identification and collection of debt	Six years	Securely disposed of

Contract management		
All records relating to the management of contracts under seal	12 years	Securely disposed of
All records relating to the management of contracts under signature	Six years	Securely disposed of
All records relating to the monitoring of contracts	Six years	Securely disposed of
School fund N/A		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Six years	Securely disposed of
School meals		
Free School meals registers	Child's 25 th birthday	Securely disposed of
School meals registers	Child's 25 th birthday	Securely disposed of
School meals summary sheets	Six years	Securely disposed of

Retention of other School records

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

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

Type of file	Retention period	Action taken after retention period ends
Property management		
Title deeds of properties belonging to the School	Permanent	<u>Transferred to new owners if the building is leased or sold</u>
Plans of property belonging to the School	For as long as the building belongs to the School	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the School	Expiry of lease, plus six years	Securely disposed of

Records relating to the letting of School premises	Six years	Securely disposed of
Maintenance		
All records relating to the maintenance of the School carried out by contractors	Six years	Securely disposed of
All records relating to the maintenance of the School carried out by School employees	Six years	Securely disposed of
Operational administration		
General file series	Six years	Securely disposed of
Records relating to the creation and publication of the School brochure and/or prospectus	Six years	Securely disposed of
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year plus one year	Securely disposed of
Newsletters and other items with short operational use	Current academic year plus one year	Securely disposed of
Signing in system for visitors	Six years	Securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Six years	Securely disposed of

Storing and protecting information

The DPO, Tim Pinto of The e-Safety Office, will undertake a risk analysis to identify which records are vital to School management and these records will be stored in the most secure manner.

The IT Manager, First Class ICT Support Ltd will conduct a back-up of information on a weekly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

Where possible, backed-up information will be stored off the School premises, using a central back-up service operated by First Class ICT Support Ltd.

Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records are not left unattended or in clear view when held in a location with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

Where data is saved on removable storage or a portable device, the device is kept in a locked, drawer or safe when not in use.

Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted by First Class ICT Support Ltd.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the School enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors do not use their personal laptops or computers for School purposes.

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

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

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

Before sharing data, staff always ensure that:

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

All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

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

The physical security of the School's buildings and storage systems, and access to them, is reviewed termly by the Caretaker in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the Head Teacher and extra measures to secure data storage will be put in place.

The School takes its duties under data protection seriously and any unauthorised disclosure may result in disciplinary action.

The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Any damage to or theft of data will be managed with support from Kirklees Emergency Planning and the DPO.

Accessing information

St. John's C.E. (C) Primary School is transparent with data subjects, the information we hold and how it can be accessed.

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

- Know what information the School holds and processes about them or their child and why.

- Understand how to gain access to it.

- Understand how to provide and withdraw consent to information being held.

- Understand what the School is doing to comply with its obligations under the GDPR.

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

Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

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

Information audit

The DPO conducts information audits on an annual basis against all information held by the School to evaluate the information the School is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

The DPO is responsible for completing the information audit. The information audit will include the following:

The School's data needs

The information needed to meet those needs

The format in which data is stored

How long data needs to be kept for

Vital records status and any protective marking

Who is responsible for maintaining the original document

The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

Once it has been confirmed that the information is accurate, the DPO will record all details on the School's Data Inventory or Information Asset Register.

The information displayed on the Data Inventory or Information Asset Register will be shared with the Head Teacher to gain their approval.

Disposal of data

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

Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be wiped clean and, where possible, cut.

Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

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

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

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

Inclusion and Equality

In line with our Equality Policy and Accessibility Plan we are committed to providing an environment that is transparent and accessible by all. Each child, staff member and parent/carer is valued, respected and challenged regardless of race, gender, religion, social background, culture or disability.

Policy Monitoring and Review

This policy will be reviewed as part of the three-year cycle or when there are significant changes warrant it. It may also be reviewed earlier should it no longer comply with school practice or the legal requirements of schools.

Policy produced by ..Sarmilla Dhangar..... Date: ..04.09.2023

Approved by (Chair of Governors): Date :

Review Date: June 2024

If you need further copies of this document, or would like the document in another format, such as enlarged print, audio tape or another language, please contact Sarmilla Dhangar, Bursar, at the school.

Telephone: 01924 325323

Email: office@stjohnsdewsbury.co.uk