Updated: February 2026

Cornerstone Academy Trust

Document Retention and School Records Management Policy

Updated: February 2026

Cornerstone Academy Trust School Records Management Policy

The school recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

Scope of the policy

This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

Responsibilities

The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher.

The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the school's records management guidelines.

Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

The 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; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the Trust's current practice, the requirements of current legislation and best practice and guidance. 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. The Trust may also vary any parts of this procedure, including any time limits, as appropriate in any case.

Data Protection

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000. Data will be stored and processed to allow for the efficient operation each School. The Trust's Data Protection Policy outlines its duties and obligations under the GDPR.

Retention Schedule

Information (hard copy and electronic) will be retained for at least the period specified in the retention schedule (below). When managing records, the Trust will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by the Trust Business Manager. Electronic records will be regularly monitored by the School Business Manager. The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

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 where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted. The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Trust Business Manager. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

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 other digital media or cloud storage. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Responsibility And Monitoring

The CEO has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with each School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to the Leadership Team. Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

The Leadership Team 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.

Updated: February 2026

Retention Schedule

FILE DESCRIPTION	RETENTION PERIOD
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
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	2 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 (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for 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 and training records	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
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 • Records of compliance with WTR	• Two years from the date on which they were entered into • Two years after the relevant period
Disciplinary and training records	6 years after employment ceases
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.
Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	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	No longer than necessary
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
School Development Plans	3 years from the life of the plan
Professional Development Plans	6 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
Health and Safety Records	
Health and Safety consultations	Permanently

Health and Safety Risk Assessments	3 years from the life of the risk assessment
Any reportable accident, death or injury in connection with work	For at least twelve years from the date the report was made
Accident reporting	Adults – 6 years from the date of the incident Children – when the child attains 25 years of age.
Fire precaution log	6 years
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Pupil Records	
Admissions records	1 year from the date of admission
Admissions register	Entries to be preserved for three years from date of entry
School Meals Registers	3 years
Free School Meals Registers	6 years
Pupil Record	Records transferred to new school when pupil leaves. If the child does not move to another educational setting (e.g. Home Schooled) then the records will be retained until the child turns 25.
Attendance Registers	3 years from the date of entry
Special Educational Needs files, reviews and individual education plans (this includes any statement and all advice and information shared regarding educational needs)	Records transferred to the new school when pupil leaves. If the child does not move to another educational setting (e.g. Home Schooled) then the records will be retained until the child turns 25.

Child Protection Records	The Child Protection records will be passed to the new school (separately from the main pupil record) when the child leaves the school. The school will ensure safe transit and obtain confirmation of receipt. The school will retain a copy of the Child Protection records until such a time that the new school acknowledges receipt of the original file. The copy will then be shredded.
Microsoft 365 Pupil Profiles	Once a pupil leaves, their Microsoft 365 account is deleted after 28 days. If required, Microsoft can restore the account for a further 30 days. After this period, all associated data is permanently deleted and cannot be recovered