



THE DEANERY

Church of England High School and Sixth Form College

DATA RETENTION

The school has a responsibility to maintain its records and record keeping systems. When doing this, the school 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
- 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 school's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the school 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 school 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 UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the school. The School's Data Protection Policy outlines its duties and obligations under the UK GDPR.

Retention schedule

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

Paper records will be regularly monitored by the Director of Business and Finance.

Electronic records will be regularly monitored by the Network Manager.

The schedule is a 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 will 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 wastepaper merchant. All electronic information will be deleted.

The school maintains a database of records which have been destroyed and Authorising Officer. 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

- Name of 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 Business Support Officer (HR & Administration). 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
- Name of 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 media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

Responsibility and monitoring

The Director of Business and Finance has primary responsibility for implementing this policy. The Data Protection Officer – Judicium Consulting Limited – Lead Contact – Craig Stilwell email – dataservices@judicium.co.uk in conjunction with the 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 management.

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.

RETENTION SCHEDULE

File description	Retention period
Employment Records	
Job applications and interview records of unsuccessful candidates	9 months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their applications 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	2 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 6 years after employment ceases
Annual leave records	6 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: <ul style="list-style-type: none"> • Opt out forms • Records of compliance with WTR 	<ul style="list-style-type: none"> • 2 years from the date on which they were entered into • 2 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	<p>10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review.</p> <p>Malicious allegations should be removed.</p>

Financial and Payroll	
Pension records	12 years
Retirement benefits schemes – notifiable events (e.g. 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	
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	
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 books	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 (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 3 years from date of entry
School Meals registers	3 years
Free School Meals registers	6 years
Pupil record	DOB +25 years
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)	Until child turns 25.

Emails	
Emails	3 years from date of sending