



Leintwardine Endowed C.E. Primary School

Record Keeping and Retention Policy

The school needs to create and maintain accurate records in order for it to function. The policy for managing records at Leintwardine Endowed C of E Primary School has been drawn up in conformity with legislation, regulations affecting schools and best practice as publicised by the Records Management Society of Great Britain.

This policy sets out guidelines for recording, managing, storing and disposing of data, whether they are held on paper or electronically in order to assist staff, and the School, to comply with the General Data Protection Regulation (2018) and the Freedom of Information Act 2000 (FIA). It should be read and used in conjunction with the following school policies and documents:

Members of staff are expected to manage their current record keeping systems using the Retention Policy and to take account of the different kinds of retention periods when they are creating new record keeping systems.

Benefits of the Retention Policy : There are a number of benefits which arise from the use of a complete Retention Policy:

- Managing records against the Retention Policy is deemed to be “normal processing” under the GDPR (2018) and the Freedom of Information Act 2000. Provided members of staff are managing record series using the Retention Policy they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a subject access request (SAR) has been made.
- Members of staff can be confident about destroying information at the appropriate time and in a secure manner.
- Information which is subject to Freedom of Information and GDPR legislation will be available when required.
- The school is not maintaining and storing information unnecessarily.

Current Pupil Records

A manilla file is kept on each pupil in a locked filing cupboard within the school office. The file holds hard copies of information about that pupil e.g. school reports, reports from external agencies, copies of letters.

The information held on the school's electronic database SIMS is provided by parents on admission. Information includes: the pupil's name, address, house, emergency contact details, free school meals status, statutory test results and daily attendance. Confidentiality of personal information is protected in accordance with the BCPS Management Information Systems and Data Protection Policy.

Pupils with Special Educational Needs

The names of pupils with special educational needs are recorded in SIMS and information regarding these individual pupils are made available to those staff with a need to know that information. Electronic copies of documents are stored, securely, on the staff server managed by our SENCO. Paper copies of documents are stored, securely, in a locked filing cabinet in the SENCO office and also within pupils' manilla folders. Increasingly these are being moved over to electronic form.

Pupils receiving Pupil Premium (PP) funding / Looked After Children (LAC) / Military funding

The names of pupils in receipt of additional funding due to their PP, LAC, post-LAC or military family status are recorded in SIMS. Information regarding these individual pupils are made available to staff with a need to know that information. Electronic copies of PP review / LAC review documents are stored on the staff server managed by the Headteacher. Paper copies of review documents are stored within pupils' manilla folders.

Medical Records Information regarding medical needs is provided by parents / carers on admission. Information provided includes any significant known drug reactions, major allergies and notable medical conditions. This information is available to staff likely to administer medication or treatment. This information is shared with external providers (trips) or external bodies (caterers) only with parental permission.

All students who have a more serious level of medical need (e.g. diabetes, anaphylaxis) have an individual Health Care Plan (HCP) which is put together by the parents/guardian with the GP's/consultant's instructions for care within school should the event arise.

The HCPs are then checked by our SENCO and stored securely on the staff server. These records will be shared with school staff to ensure pupil safety. The photographs of children (for whom parents have given permission) will be displayed in the staff room to help identification. The Headteachers hold the original copies in a locked cabinet in their office. These records are shared with the medical services in case of emergency.

Financial Records

The finance and office staff have access to information regarding school dinner payments and school trip payments.

Access by Staff All teaching and office staff are able to access the school's password protected database (SIMS). Teaching staff may consult the pupil records held in the School Office including emergency contact phone numbers. Other data e.g. discretionary absence request letters / attendance letters etc. are stored securely and only available to the necessary staff on request.

Data Protection Policy Parents accept a place for their child at Leintwardine Primary School in the knowledge that data about pupils and their parents will be collected on admission to allow for the efficient operation of the school. This data will be updated regularly and stored/ processed in order with the GDPR (2018) rules for good information handling.

Staff Induction. All new teaching and office staff will be given training on accessing and managing school records to ensure compliance with these retention time scales. As a guiding principle, GDPR requires that personal data is only retained for as long as necessary - that is, necessary for the specific lawful purpose (or purposes) it was acquired. Any information which is held is to be kept in accordance with BCPS' Management Information System and Data Protection Policy.

Retention Periods - The table at the end of this policy provides guidance on retention periods for different records held by Leintwardine Primary School. Unless there is a specific statutory obligation to hold or destroy records, the retention periods are established by the school for guidance purposes.

Disposal of Data

When information is no longer required, it can be disposed of. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Skips and 'regular' waste disposal are not considered to be secure.

Paper records should be disposed of in the confidential waste bin in the administration area. If this is not possible it should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely.

1. Child Protection The retention and use of records relating to child protection matters concerning pupils, and child protection allegations against staff requires specific guidance in this schedule.

Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
Child Protection files	Yes	Until child leaves BCPS then transfer to the new education provider	DO NOT DESTROY ANY RECORDS	
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded		Until the person's normal retirement age, or 10 years from the date of the allegation if that's longer	SHRED	<p>ICO Employment Practices Code: Supplementary Guidance 2.13.1 (Discipline, grievance and dismissal)</p> <p>“Records of allegations about workers who have been investigated and found to be without substance should not normally be retained once an investigation has been completed. There are some exceptions to this where for its own protection the employer has to keep a limited record that an allegation was received and investigated, for example, where the allegation relates to abuse and the worker is employed to work with children or other vulnerable individuals”.</p> <p>Summary record to be retained on confidential personnel file, and a copy given to the person concerned.</p>

2. Governors & School Committee Meetings				
Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
Instrument of Government including articles of association	No	Permanent	Archive	Stored on SERVER - Office – Governors
Get Information About Schools	Yes	Retain during governor’s term of office. Update termly.	DELETE	
Governors minutes – principle set signed with appropriate agenda & any reports referred to	Confidential minutes	Permanent	Archive	Stored on SERVER – Office - Governor’s folder. Confidential minutes locked into HT office. Copy of last 5 years to be kept in files in headteachers office in folder.
Governors eligibility forms, training logs and pecuniary interests forms	Yes	Retain during governors term of office	Shred	Stored SERVER – OFFICE - Governors
Governor documentation - agendas, action plans and policy documents	No	Date of meeting +3 years	Shred	Server – Office - Governors
Governor reports	No	Date of meeting + 6 years	Shred	Server – Office – Governors
Meeting papers relating to Annual Parents’ Meeting	No	Date of meeting + 6 years	Secure disposal	

Records relating to complaints dealt with by the Governing Body	Yes	Date of the resolution of the complaint + a min of 6 years	Secure Disposal	
Annual Reports	No	Date proposal accepted or declined + 3 years	Secure Disposal	

3. Staff Records				
Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
Staff Personnel files	Yes	7 years from when staff member leaves	SHRED	Within 6 months of staff member leaving all documentation should be stored on SERVER – Office – Personnel folder (no paper copies to remain)
Staff historic allegation files	Yes	10 year from allegation or normal retirement age (whichever is longer)	SHRED	Within 6 months of staff member leaving all documentation should be stored on SERVER – Office – Personnel folder (no paper copies to remain)
Staff appraisal files	Yes	5 Years	SHRED	By October, following academic year – all docs should be stored SERVER – SMT – Appraisal – Individual folders
Emergency contacts folder - staff	Yes	Updated annually or as needed and previous records removed.	Shred	Only latest copy to be retained
Appointment documents, unsuccessful candidates	Yes	6 months	Shred	Ensure all emails / files stored electronically are deleted after interview / selection date.
Trainee Teacher records	Yes	All copies to be deleted at end of placement and submission of final report; except final report to be kept by mentor / HT for 3 years (may be required for references) and then deleted.	SHRED/ DELETE	Ensure all electronic documents removed by mentor / class teachers etc. Teacher training college to provide BCPS / student with user agreement re. data
Professional Development Plans	Yes	Life of the Plan + 6 years	Secure Disposal	
School Development Plans	No	Life of the Plan + 6 years	Secure Disposal	

4. Pupil Information				
Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
EHA records / CAF / TAF	Yes	Retain for 6 years after plan created. Staff to delete from own PC / memory stick annually.	SHRED	Ensure each updated copy is signed and copy stored in manila folder and in central file on office shared server – Office- safeguarding- individual pupils
Books, folders & test papers	Yes	Send books / papers home and shred test papers after 1 year	SHRED / SEND HOME	Shred front page of test papers – remainder can be recycled
Pupil Premium tracking documents / passports. LAC tracking.	Yes	Sent with child to next school	SHRED / DELETE	Ensure each updated copy is signed and copy stored in manila folder and in central file on office shared server.
Pupil manilla folders	Yes	Pupil manila folders	SEND TO NEXT SCHOOL	Only latest copy to be retained
Behaviour slip book / record	Yes	2 years after incident	Shred	Copies of letters re. behaviour slips to be stored in manila folders.
Emergency pupil contacts register & medical list	Yes	12 months	SHRED/ DELETE	
Intimate care plans / Manual handling risk assessments	Yes	Retain for 6 years after plan created	SHRED/ DELETE	Within 3 months of child leaving all documentation should be saved in SEND – individual pupil folder – Office – SEN – Individual Pupil
Medical Health Assessments including dietary assessments	Yes	Updated termly unless changes warrant this sooner. Latest copy retained until child has left the school.	SHRED/ DELETE	
Special Educational Needs files, reviews and Individual Education Plans	Yes	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.

5. Curriculum				
Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
Data Tracker FTT aspire	Yes	1 year beyond pupil leaving school	Deleted by FTT Aspire	FTT Aspire GDPR Compliant
Data Tracker NCA Tools	Yes	1 year beyond pupil leaving school	Deleted by NCA Tools	Ensure NCA Tools GDPR Compliant
Data Tracker Perspective Lite	Yes	1 year beyond pupil leaving school	Deleted by Perspective Lite	Ensure Perspective Tools GDPR Compliant
Class Dojo	Yes	1 year beyond pupil leaving school	Deleted by Clasd Dojo	Ensure Class Dojo Tools GDPR Compliant
Purple Mash	Yes	1 year beyond pupil leaving school	Deleted by IT manager	Ensure Purple Mash GDPR Compliant
Bikeability	Yes	End Of Training	SHRED/DELETE	Ensure Bikeability GDPR Compliant

6. SLT/ Office Records				
Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
Behaviour/ antibullying logs	Yes	7 years		Behaviour log on server – Shared- Staff – Behaviour.
Accident and Incident Logs	Yes	7 years after incident for adults; 25 years after birth for children	SHRED	
First Aid books	Yes			
Emergency contacts folder - pupil	Yes	Update annually at least	SHRED	
Medicine administration records	Yes	1 year beyond pupil leaving school	SHRED	
Physical restraint log	Yes	25 years from DOB for child.	Shred	Bound book – kept in Office filing cabinet
Evolve School Trip Records including trip risk assessments and pupil lists	Yes	Paper copies to be shredded on return except copy in HT office to be kept for one year.	Deleted by Evolve SHRED/ DELETE	Ensure Evolve GDPR compliant
Bus Register	No	Replace weekly as long as no incidents	SHRED	
Visitor signing in and out sheets	Yes	5 Years	SHRED	
Signing in and out and Late Book (Pupils)	Yes	1 Year	SHRED	
Parental Absence request Form	Yes	3 Years	SHRED	
Permission Forms	Yes	Until Event has occurred without issue	SHRED	
Catering returns	Yes	1 year	SHRED	Ensure Caterer GDPR compliant
Admission documentation, parent correspondence	Yes	Delete when processes via SIMS or matter resolved	SHRED	Ensure SIMS GDPR compliant
HT Attendance Monitoring Folder	Yes	3 Years	Delete	Server – Office – Attendance - Letters

6. SLT/ Office Records (cont)				
Basic file description	Data Protection Issues	Retention Period	Action at the end of the administrative life of the record	
HT Data Folder	Yes	7 years		Behaviour log on server – Shared- Staff – Behaviour.
HT Key Information Folder	Yes	7 years after incident for adults; 25 years after birth for children	SHRED	
Single Central REcord	Yes	permanent - Continual update		
DBS NUMBER	Yes	Number to be on SCR but no copy of certificate kept		
Leave of Absence Request	Yes	3 Years	SHRED/ Delete	
Images of Staff an pupils stored on SIMS	Yes	Current academic year if permission given	Delete	
SIMS	Yes	1 Year after left (TBC)	Delete	Ensure SIMS GDPR compliant
Emails	Yes		Delete	