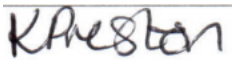
Policy/Procedure Name:	RETENTION (OF DATA) POLICY		
Last Update:	**August 2024**	Next Update Due:	**August 2027**

Author	**Alex Smythe**
Signature of Authorised Individual	
Signature of the Director	

Contents

1.1 Introduction

This record retention and deletion policy contains recommended retention periods for the different record series created and maintained by Willow Park School. The schedule refers to all information regardless of the media in which it is stored. The schedule is contained in paragraph 1.11 of this policy.

Some of the retention periods are governed by statute. Others are guidelines, following best practice, employed by schools throughout the United Kingdom. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation 2018 (GDPR), the Data Protection Act 2018 (DPA), Article 8, the Human Rights Act 1998, the Freedom of Information Act 2000 (FOI) and the Code of Practice on Records Management (under Section 46 of the FOI).

Managing records series using these retention guidelines will be deemed to be 'normal processing' under the terms of the legislation noted above. If those record series are to be kept for longer or shorter periods than the time scales held in this document, the reasons for any deviation must be recorded.

This policy will be reviewed at intervals of no less than three years, or exceptionally, if required by changes in Data Protection, Freedom of Interest or other legislation, where relevant.

1.2 Purpose

All schools need to create and maintain accurate records for them to function and carry out the tasks of educating and safeguarding pupils. This policy, for managing records at Willow Park School, has been drawn up in conformity with legislation, regulations affecting schools and best practice as promoted by the Information and Records Management Society of Great Britain.

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

- Management Information Systems
- Data Protection (GDPR) Policy
- Privacy Notices

The implementation of the General Data Protection (2018) did not fundamentally change the principles around the duration of records retention. However, it has introduced stricter rules about the use and storage of personal data, requiring more dynamic, efficient and secure storage systems. It is expected that;

- All information held by schools needs to be justifiable, by reference, to its purpose.
- Schools must be transparent and accountable as to what data they hold.
- Schools must understand and explain the reasons why they hold data.
- Schools must be able to respond to Subject Access Requests.
- Schools must be able to amend, delete or transfer data promptly upon any justified request.
- Schools must be able to audit how personal data was collected and when and why.
- *Schools must hold sensitive data securely, accessed only by those with reason to view it and possess a policy as to why it is needed.*

All members of staff, with access to records, are expected to;

- Manage their current record keeping systems using the Retention Policy.
- Only dispose of records in accordance with the requirements outlined in this policy, if authorised to do so.
- Ensure that any proposed divergence from the records retention schedule and disposal policies is authorised by the Head Teacher or Principal.

This policy does not form part of any employee's contract of employment and is not intended to have a contractual effect. However, it does reflect the school's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the school but 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 the procedure, including time limits, as appropriate.

1.3 Why hold a Retention Policy?

There are a number of benefits which arise from the use of a 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). Where members of staff are managing records using the Retention Policy, they will not be culpable of tampering or the unauthorised alteration of data, once a Freedom of Information request or Subject Access Request (SAR) has been made.
- Members of staff can be confident about destroying information at the appropriate time and in a secure fashion.
- Information which is subject to Freedom of Information and GDPR legislation will be available, when required.
- The school is not maintaining and holding information unnecessarily.

1.4 Examples of How Pupil Records May Stored and the Information Shared.

The following examples illustrate a number of options by which schools may hold data – in some cases, where information is held on different platforms, a combination of these options may be employed ('hybrid files'). It is advised that the school, working with their Data Protection Officer, creates a summary of what information they hold and how;

- Pupil record (hard copy) - 'a manila file is kept on each pupil, in a locked filing cabinet in the office. This file holds hard copies of information about that pupil e.g. consent forms, annual data audits.'
- Pupil record (electronic) - 'a record is held on the school's electronic Management Information System (Horizons and Tapestry) from information provided by the child's parents upon admission. Information includes; pupil name, address, emergency contact details, free school meal status, ethnicity, statutory test results, daily attendance'
- Pupils receiving Pupil Premium (PP) funding/Looked After Children (LAC) – 'pupils in receipt of additional funding, due to their PP, LAC or post-LAC family status, are recorded in the Management Information System (Horizons). Information regarding individual pupils is made available to involved staff, with permissions delegated and recorded by the HT. Electronic copies of PP review/LAC review documents are held, securely, on the

appropriate staff drive within the server. Hard copy information is stored within the pupil's manila folder.'

- Medical Records – 'information regarding the medical needs of a pupil is provided by parents/carers upon admission and updated, where necessary, following the annual data check. Information provided includes any significant known reactions to medication, major allergies and notable medical conditions. This information is available to staff likely to administer medication or treatment. The information is shared externally (trips) or to external agencies (catering) only with parental permission. This is information is held under the terms of the retention schedule, following the completion of the trip, or, with regards catering, for the duration of the child's time in school.
- Any pupil who has a more serious level of medical need (e.g. diabetes, anaphylaxis) will have an individual Health Care Plan (HCP), which is presented by the parent/guardian, with the GP's/consultant's instructions for care within the school should the need arise. These records, with the consent of the parent/guardian, will be shared with school staff to ensure pupil safety. Photographs of the children (where appropriate and applicable), will be displayed in the school. Hard copy information is stored with the pupil's manila folder. These records are shared with medical services, in the event of an emergency and any visible instructions/guidance relating the child will be displayed only for the duration of their time in school.'
- Financial Records – 'financial records are held in the business office.

1.4.1 Emails, Texts and Instant Messaging

Emailing is a form of communication – it is not a means of storing information that may be kept securely elsewhere. Emails should not be kept, but rather transferred, if the information they hold falls into the categories listed within the Retention Schedule e.g. does it form part of the pupil record? Does it relate to an employee or a decision about an employee? If so, this information could be transferred e.g. printed off and kept in the pupil's manila folder, and the email deleted. Emails and attachments which hold data must not be kept as emails; they must be either be saved in an appropriate electronic management information system or printed off and filed as a hard copy document.

At Willow Park, we do not implement a rule whereby emails are automatically deleted after a period of time. Such a rule would limit the amount of information that might be available to a data subject under a Subject Access Request.

Similarly, texts, Instant Messages (e.g. WhatsApp, Facebook Messenger) or message boards and forums are not considered a permanent record of being ephemeral and temporary. If the content of the message or text is significant e.g. a staff member highlights concerns around a pupil's behaviour, then it should be copied and transferred into the appropriate filing system e.g. a safeguarding case file, either by saving it in a readable electronic format, or printing it off, or taking a screen shot.

Any information recorded within texts, Instant Messages, message boards or forums is subject to the same Data Protection and Freedom of Information legislation, regardless of format. Therefore, it is advisable to only use these methods of communication to transmit information which is not sensitive or directly related to a third party. Similarly, with regards emails, all electronic communications, whilst they are held by the school, are disclosable under the same legislation and anything written or held, within an email, could potentially be made public under the terms of a Subject Access Request.

1.4.2 Social Media

It should be noted though that social media is not just a means of communication, but can also act a repository for storing information and third party data. Information held in this format is subject to the Freedom of Information Act 2000 and the Data Protection Act 2018.

Social media outlets have different retention periods. Schools must be aware of how long these periods are, outline this within their Data Protection Policy and secure the appropriate consent to share personal data to enable the rights of the data subject. The school needs to ensure that the primary users (i.e. those staff members who hold administrative permissions, to upload and remove information) are aware of these retention periods. Where these retention periods are longer than that set out as part of a standard school policy or best practice e.g. removing pupil images from the school's website when that pupil has left, processes must be in place to remove any posts or photographs on a regular and routine basis.

Social media posts can remain online for a period long after the school has deleted them. They can be shared and redistributed many times, beyond the control of the individual who first posted them. There it is vital that the school is clear when obtaining the consent to share data, from pupils, parents, staff and volunteers, as to where information will be shared, for how long and outlining the risk of information being shared, or cached, beyond their control.

1.5 Access to Records

For the efficient running of the school, all teaching staff and relevant office staff will have access to the school's Management Information System (Horizons). Teaching staff may complete some the following functions e.g. enter names on the register or add other agency involvement, and may consult the pupil record. N.B. where records are maintained as hard copy within the school office, access is available to teaching staff with regards some information e.g. emergency contact numbers, consents. Other information e.g. discretionary absence request letters, attendance letters, are held in the school office and are only available to the relevant member of staff upon request.

All permissions to access data are granted by the Head Teacher / Principal and recorded in the member of staff's personnel file.

All teaching and office staff will be given training and guidance on accessing and managing school records, to ensure compliance with the time scales laid out under the retention schedule. As a guiding principle the General Data Protection Regulation requires that personal data is only retained for as long as is necessary and for the specific lawful purpose(s) it was acquired; all information, held by the school, must be kept in accordance with the school's Data Protection Policy.

1.6 Data Protection Policy

Pupils, parents and member of staff are informed, via the school's Data Protection Policy, that any information held on them, upon either admission or commencement of employment, is for the school to carry out statutory functions, necessary for the efficient operation of the setting – data held will be reviewed regularly and will be stored, processed and shared (where appropriate and applicable) under the terms of the General Data Protection Regulation (2018).

1.6.1 Retention Periods

The following tables provide guidance on retention period for the different records held by Willow Park School. Unless there is a specific statutory obligation to hold or destroy records.

1.6.2 Disposal of Data

As mentioned above, the fifth Data Protection principle, states that 'Personal data processed for any purpose, or purposes, shall not be kept longer than is necessary for that purpose, or purposes'. It is the responsibility of the Head Teacher that records, which are no longer required for business use, are to be reviewed as soon as possible, so that the appropriate records can be destroyed or transferred, where necessary.

Not all data needs to be destroyed. The school will determine whether records are to be selected, either for permanent preservation, or for destruction or to be transferred into a different format e.g. digitised, or to be retained further, by the setting, for research or litigation purposes. Any decision, regards a change to the way data is held in the setting, must be documented as part of the records management policy. For example; financial records can be destroyed after six years, plus the year they were created in, and are often shredded or passed to a confidential waste provider for safe destruction.

When information is no longer required, it should 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. It is recommended that paper documents are destroyed with a cross shredder – where this is not possible, and, e.g. a ribbon shredder is employed, the waste should not be recycled but destroyed beyond recognition e.g. via an incinerator bin.

Skips and 'regular' waste disposal are not considered to be secure.

CD's/DVD's/discs should be cut into pieces. Hard copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal companies are employed, they should, wherever possible be supervised and any destruction of data or removal of data, from the site, is logged and the destruction certified.

Destruction of data will be planned with specific dates and all records will be identified as to the date of destruction. N.B. if a record is noted pending destruction or transfer, either to archives off site or to another setting, but has not yet been destroyed/transferred, and a request for records has been received, that record must still be made available to the requestor.

The Freedom of Information Act 2000 requires the school to maintain a list of all records that have been destroyed and who authorised their destruction. The appropriate members of staff (Data Lead) should record;

- File reference and/or unique identifier
- File title or brief description of contents
- Number of files
- Name of the authorising officer

1.7 Transfer of Records to Archives

Where records have been identified as being worthy of permanent preservation, due to their historical or social value, they wiil be retained on site.

1.8 Transfer of Records 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 (e.g. digital or virtual, 'cloud' based). The lifespan of the media, and the ability to migrate data, will always be considered.

1.9 Transfer of Records to other Settings

When a child leaves the school, all pupil records will be transferred in a secure manner, to the child's new school. If the records contain sensitive information (e.g. Child Protection records), proof of receipt will be obtained and logged by the school's Data Lead. All data held by the school will then be deleted, including all paper records and data stored electronically. A record will be kept for tracking and auditing purposes only.

1.10 Responsibility and Monitoring

The Head Teacher is tasked with the role of Data Lead and holds primary and day to day responsibility, for implementing this policy. The Princiapl is responsible for monitoring its use and effectiveness and resolving any queries with regards the interpretation of the policy. The Data Protection Officer will consider the suitability and adequacy of this policy and will pass any amendments or alterations directly to the Principal.

Internal control systems and procedures will be subject to regular audits, to provide assurance that they are effective in creating, maintaining and removing records.

1.11 Outline Retention Schedule

There follows an adapted version of the IRMS pro forma retention schedule. This offers a comprehensive and thorough review of all possible data that may be held by a school.

1.11 – Retention Periods

Please note that any record containing pupil information may be subject to the requirements of the IICSA. The school will implement any instruction which has been received from IICSA. The instructions from IICSA will override any guidance given in this Retention Schedule.

1.11.1 Employment Records	
FILE DESCRIPTION	**RETENTION PERIOD**
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	2 years after the termination of employment
DBS checks and disclosures of criminal records forms	The school does not have to keep copies of the DBS certificates. If the school does though, the copy must not be retained for more 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 then up to 6 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	While employment continues and then up to 6 years after employment ceases
Allegations of a child protection nature against a member of staff including where the allegation is founded	DO NOT DESTROY (Refer to note on front page) then until the person's normal retirement age or 10 years from the date of allegation, whichever is longer, then review. NB – allegations that are found to be malicious should be removed from personnel files, from the date they are proven to be unfounded.

1.11.2 Financial and Payroll Records	
FILE DESCRIPTION	**RETENTION PERIOD**
Pension records	Current year + 6 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	Current year + 6 years
Payroll and wage records	Current year + 6 years
Maternity/Adoption/Paternity Leave records	Current year + 3 years
Statutory Sick Pay	Current year + 3 years

1.11.3 Agreements and Administration Paperwork	
FILE DESCRIPTION	**RETENTION PERIOD**
School Improvement Plans	Life of plan + 6 years
Professional Development Plans	Life of the plan + 6 years
Visitor management systems (including electronic systems, visitors' books and signing in sheets)	Current year + 6 years
Newsletters and circulars to staff, parents and pupils	Current year + 1 year

1.11.4 Health and Safety Records	
FILE DESCRIPTION	**RETENTION PERIOD**
Health and Safety Policy Statements	Life of the policy + 3 years
Health and Safety Risk Assessments	Life of the assessment + 3 years
Any reportable accident, death or injury in connection with work	Date of the incident + 3 years
Accident reporting	Adults – Retain for 7 years from the date of the accident Children – Retain for 25 years from the child's date of birth
Fire precaution log books	Current year + 3 years
Process of monitoring: - · radiation · asbestos · 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

1.11.5 Pupil Records	
FILE DESCRIPTION	**RETENTION PERIOD**
Admissions records	Up to seven years from the date of admission
Register of Admissions	Entries to be preserved for seven years from date of entry
School Meals Registers	Current year + 3 years
Free School Meals Registers	Current year + 6 years
Pupil Record	Rretain whilst the child remains at school / Date of birth of the pupil + 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)	Retain from date of birth of the pupil + 31 years

Appendix A – List of School Records and Data safely destroyed

Specimen Checklist for Annual Review of School Records and Safe Data Destruction

The following sheet can be completed or, alternatively, document in a spreadsheet

Reference Number	File/Record Title	Description	Reference or Cataloguing Information	Number of Files Destroyed	Method of Destruction	Confirm; (i) Safely Destroyed (ii) In accordance with Data Retention Guidelines **Yes/No**	Name of Authorising Officer
e.g.	School invoices	Copies of purchase invoices dated 2023/12	Folders marked 'Purchase Invoices 2023/13' 1-3	3 Folders	Cross shredded	Yes	K Preston (Head)
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							

Appendix B - Safe Retention of Records Information Security and Business Continuity

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with Data Protection legislation. Taking measures to protect your records can ensure that:

• Willow Park can demonstrate compliance with the law and avoid data loss incidents;

• In the event of a major incident, the school should be able to stay open and will at least have access to its key administrative and teaching records.

Our Information Security Policy should incorporate a Business Continuity Plan and should deal with records held in all media across all school systems:

• Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images)

• Hard copy (including but not limited to paper files, plans)

B1 Digital Information

In order to mitigate against the loss of electronic information, we:

a. Operate an effective back-up system

- We undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Data is stored in the cloud. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible. The location of the cloud storage and the security offered are appropriate for the information and records stored.

b. Control the way data is stored within the school

- Personal information should is **not** stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff are advised not to hold personal information about pupils or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

c. Manage the location of server equipment

- We ensure that the server environment is managed to prevent access by unauthorised people.

d. Ensure that business continuity plans are tested

- We test restore processes on a regular basis to ensure that the first time we identify a problem with the backup is not the first time we need to retrieve data from it.

B2 Hard Copy Information and Records

Records which are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access. Wherever possible, and where appropriate, if information can be stored electronically rather than hard copy, we store it electronically.

a. Fire and flood

- The cost of restoring records damaged by water can be high but a large percentage may be saved; a fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all vital information is stored in filing cabinets, drawers or cupboards; metal filing cabinets, because they are a good first level barrier against fire and water.
- Where possible vital records should not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be seriously damaged (possibly beyond repair) in the event of a flood.
- Physical records should not be stored on the floor.

b. Unauthorised access, theft or loss

- Staff are asked not to take personal data on staff or pupils out of the school unless there is no other alternative. Confidential ecords held within the school should are in lockable cabinets. Access to the office, in which personal information is being worked on or stored, is restricted to school staff. All archives or records storage areas will be lockable and have restricted access.

c. Clear Desk Policy

A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/or flood damage.

In the school office at Willow Park, we operate a clear desk policy. This involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

B3 Risk Analysis

The school's leaders will undertake a business risk analysis to identify which records are vital to school management and these records should be stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks.

B4 Responding to Incidents

In the event of an incident involving the loss of information or records the school will pull together an incident response team (Head, Principal, Business Manager) to manage the situation. The process will involve the Data Protection Officer (Kimberley Preston) liaising with the Information Commissioner's Office if an information security breach needs to be reported. Staff must note that – a loss of data e.g. accidental destruction of records, is a data breach just as if those records had been lost, stolen or wrongfully shared.

B5 Maintaining a School Archive

Our school generates a large amount of data that is not necessarily personal or sensitive, yet is worthy of retention as part of the school's historical legacy; e.g. records, year photographs, fliers, letters, issues of the school newsletter. These, and other items, document not only the school's past, but also reflect its place within the greater community. Sometimes we may be asked what historical records are still maintained within the setting. These requests may come from former school pupils, when they need to provide proof of their attendance or educational record. Other requests come from family historians carrying out research on their family tree and about their ancestors.

A school archive is different from an official school records system – all schools will have an established record-keeping system for official records and a Management Information System, which includes record-keeping guidelines (as detailed in this policy). A school archive preserves data, beyond the retention period, where there is a legitimate interest in holding that information e.g. to commemorate a significant event in the life of the school. It can take on many characteristics and serve many purposes--but it neither compliments nor replaces the official record-keeping systems. However, records held in an archive must be accessed the same way, as current school records, and it would be necessary for the school to prove the identity of anyone requesting historical information, in the same way we would a Subject Access Request. To comply with the General Data Protection Regulation, the schools will consider the following, if a request has been made to consult someone else's personal information in school archive that is not in the public domain.

- Entries for an individual who is (or would be) more than one hundred years old can be viewed without restriction.
- If the individual is less than one hundred years old, the requester would need to provide proof that that person is now deceased, and to supply a death certificate for them.
- If the requester wishes to access information still held under the terms of the retention schedule, they would need to make a Subject Access Request.

When creating an archive, we will ensure that it serves the purpose of repository for the collection and preservation of historically valuable documents, relating to the history of the school or the community, which otherwise would be lost.