

Policy Title: Records Management Policy	Effective Date:	October 2022
SMT Member Responsible: Julia Finch	Review Date:	October 2024
Governors' Committee Responsible: Premises		

1. Introduction

Sheldon School (the School) recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and contribute to the effective overall management of the organisation. Records provide evidence for protecting the legal rights and interests of the School and provide evidence for demonstrating performance and accountability. The aim of this policy is to provide a framework for managing the School's information to enable the School to:

- Make informed decisions;
- Be open and transparent;
- Respond appropriately to information requests;
- Protect records;
- Comply with the legislative requirements;
- Effectively work with its partners, and share information as required;
- Demonstrate accountability.

2. Objectives

The objective of this policy is to define a framework for the School to manage data, information, and records.

3. Definitions

Data - Raw facts and figures that supply the basis for information.

Information - Data which has been collected, organised, ordered and given both meaning and context.

Record - Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations, or in the transaction of business.

Confidential Waste - See [Appendix 1](#).

4. Scope

This policy applies to all employees of the School including contract, agency and temporary staff, volunteers and employees of partner organisations working on behalf of the School

All records created, held, and maintained by the School in the course of its duties are covered by this policy. This is irrespective of the format of the information, including, but not limited to:

- Paper records
- Electronic records (Word Documents, emails, PowerPoints, database, etc.)
- Photographs, videos, etc.
- Discs

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, activities or decisions.

5. 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.

All members of staff and employees are individually responsible for the records they create or hold. Individuals must ensure that records are accurate, maintained securely, and disposed of in accordance with this policy.

6. Creation & Storage

All School staff are responsible for creating and maintaining data, information and records in relation to their work, and storing them in a way which ensures that they can be identified and retrieved when required.

Records must be appropriately stored with due regard for efficiency, cost-effectiveness, security, durability and access. Appropriate procedures and processes are in place to ensure the physical and intellectual security of School records. These are referenced in the Information Security Policy.

Storage conditions and handling processes should be designed to protect records from unauthorised access, loss, destruction, theft and disaster. This in line with the UK General Data Protection Regulation (UKGDPR) principles of data protection by design, and integrity and confidentiality.

The retention of records for longer than necessary is in breach of the UKGDPR, and the duplication of records should be limited to optimise the use of space for storage purposes and to aid data accuracy.

7. Retention and Disposal

Information held for longer than is necessary carries additional risk and cost, therefore records and information shall only be retained when there is a business or legislative need to do so. Under the UKGDPR and the Data Protection Act 2018 (DPA 2018), personal data processed by an organisation must not be retained for longer than is necessary for its lawful purpose.

The retention of specific documents may be necessary to:

- Fulfil statutory or other regulatory requirements.
- Evidence events/agreements in the case of disputes.
- Meet operational needs.
- Ensure the preservation of documents of historic or other value.
- Evidence child protection matters.

The untimely destruction of documents could cause the School:

- Difficulty in defending litigious claims
- Operational problems
- Embarrassment
- Failure to comply with the Freedom of Information or Data Protection laws.

Conversely, the permanent retention of all documents where there is no business need or other legal basis to retain them, poses regulatory and security risks, as well as being a breach of personal data.

Appropriate secure disposal is accordingly implemented at the School in accordance with the School's retention policy for the following reasons:

- To comply with the School's retention policy and data protection principles;
- To comply with Article 5 of the UKGDPR which states that personal data must not be kept in an identifiable form for longer than is necessary
- To free-up storage space (there is evidence that the de-cluttering of office accommodation can be psychologically beneficial for employees.);
- To reduce the risk of fire (in the case of paper records);
- To lessen the risk of a data breach through data loss or unauthorised access.
- To increase the efficiency of the exercising of data subject rights.

7.1 Retention Schedule

In line with all relevant legislative requirements, including the UKGDPR and DPA 2018, the School will keep some forms of information for longer than others. Information will not be kept indefinitely, unless there are specific requirements.

The School maintains records in line with the schedule included in the Information and Records Management Society's (IRMS) Toolkit for [Schools/Academies] (2019), which is found here [<https://irms.org.uk/page/SchoolsToolkit> / <https://irms.org.uk/general/custom.asp?page=AcademiesToolkit>].

7.2 Disposal

The School will either use an accredited confidential waste disposal provider or shred the information on site using a cross-cut shredder. Information on what should be deemed as confidential waste is detailed in Appendix 1.

Wherever practicable and appropriately secure, disposal methods should encourage recycling.

Electronic files are securely overwritten, in accordance with government guidance, and other media is shredded, incinerated, or otherwise disintegrated for data.

The disposal of School data, in either paper or electronic form, is conducted in a way that makes reconstruction highly unlikely. Once data has been deleted, it is deemed to be a permanent deletion, irrespective of whether it could technically be reconstructed from a back-up.

Under no circumstances should paper documents containing personal data or confidential information be simply binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties and render the School liable to enforcement action by the Information Commissioner's Office.

If records are accidentally destroyed or discovered, this should be reported as a data breach to both the School Business Manager and Network Manager, in line with the Data Breach Policy.

A destruction log is kept of all data that is disposed of. The log includes the document type (e.g. Personal data), date of destruction, method and who authorised the destruction.

7.3 Archiving

A small percentage of the School's records will be selected for permanent preservation as part of the School's archives. It is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations of former pupils and staff; and to serve as a research resource for all interested in the history of the School and the community it serves.

8. Monitoring and compliance

This policy is reviewed every 2 years.

Compliance with this policy shall be monitored through a review process undertaken by the person with overall responsibility for records management within the School. This will be achieved by an annual survey to check if records are stored securely and can be accessed appropriately.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the School, in consultation with senior management and our Data Protection Officer, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

9. Relationship with Existing Policies

Linked policies which can all be found on the school's shared drive at T:\Staff Resources\POLICIES\Word version:-

- Data Breach Policy
- Information Security Policy
- Data Protection Policy
- CCTV Code of Practice
- Acceptable Use Policy (AUP)
- Bring your own device Policy

The school has appointed I-west as its Data Protection Officer. I-west can be contacted at i-west@bathnes.gov.uk

Appendix 1 - What is Confidential Waste?

(1) Any record* which details personal information

What is personal information?

- Relates to and identifies a living person
- Could help someone identify a person when used with other information
- Is an expression of opinion about an individual
- Indicates our intentions towards an individual

Such as: Name, Address, Date of Birth, Email, Phone numbers, Location data, IP addresses

(2) Any record* which details special categories of personal data

What are the special categories of personal data?

- Racial and/or Ethnic Origin
- Political Opinions
- Religious Beliefs (or other beliefs of a similar nature)
- Trade Union membership
- Biometric Information e.g. Photos
- Mental or Physical Health condition
- Sexual life and Orientation
- Criminal Records are afforded similar protections to special category data and are similarly sensitive

Such as: Safeguarding, Accident/First Aid, Equalities information, Legal records

(3) Any record* which details business/commercially sensitive information

What is business/commercially sensitive information?

- Information which the School would be affected by any loss of, or unauthorised access to.

Such as: Contracts, opinions on service delivery, tender information.

If you have any doubt then please treat the information as Confidential

- * A Record can be in many formats – e.g. Paper, Post-it notes, Disks, CDs, Tapes, Posters, E-mails etc.