Fairhaven CE VA Primary School

GDPR
Record & Data Management Policy

Date Agreed by Staff: 13th Oct 2025

Date Agreed by Governors: 16th Oct 2025

Date for Review: Autumn 2027

Signed *R Whiles* **(Chair of Governors)**

Records and Data Management Policy

Contents

Policy Statement 3
Policy Scope 3
What data? 3
Who this policy applies to? 4
Where it applies 4
Roles and Responsibilities 4
Information Classification 5
Retention Schedules 6
Data storage, backup and destruction 6
Other relevant policies 7

Policy Statement

Fairhaven Primary School will create, maintain and manage accurate, reliable and useable records in line to ensure the school has the information it needs to operate and to have information available when it is needed.

The school will formulate an information governance framework to ensure the information in the School's electronic and paper records:

- support the successful operations of the School
- can be trusted
- contain only the minimum required information for the purpose of the information
- are properly maintained and organised
- are handled appropriately and in accordance with legal requirements and other guidance
- remain accessible, readable, authentic and up-to-date
- are kept securely, whatever the format
- can be easily found by those who need them
- only accessed by those permitted to view them
- support efficiency by avoiding duplication and only printing emails and electronic records when absolutely necessary
- are retained for a specified length of time and not indefinitely as retaining data can expose the School to risk
- are disposed of securely as per the disposal schedule

Failure to comply with this policy can expose the school to fines and penalties, failure of trust and adverse publicity, difficulties in providing evidence when we need it, responding to data subject access requests and in running our operations.

Complying with this policy helps the school comply with legislation and operate efficiently.

Policy Scope

What data?

This policy covers all data that we hold or have control over including where it is held by third-parties (e.g. cloud storage providers or offsite records storage).

This includes physical data such as:

- hard copy documents
- contracts and invoices
- notebooks & diaries
- letters
- invoices

- teacher, student and employee files
- hard copy media, including but not limited to photographs

It also includes electronic data such as:

- emails
- electronic documents
- electronic records held in databases
- audio and video recordings
- other electronic media, including but not limited to photographs
- CCTV recordings.

It applies to both personal data and non-personal data. In this policy, we refer to this information and these records collectively as “data”.

This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

Who this policy applies to?

This policy is the responsibility of all staff including:

- Employees (permanent and temporary, agency and casual staff)
- Volunteers, students, interns and trainees doing placements within the School
- Governors and Trustees
- Contractors conducting business with the School
- Any other third-parties acting jointly or in partnership with the School
-

Where it applies

Premises

- All premises operated by the School
- Anywhere that any of those listed in “Who this policy applies to” conduct their work

Systems

- Any electronic system or database operated by, or on behalf of the School
- Any computer system, peripheral equipment, software, memory devices, tablets and smartphones
- personal devices not owned by the School, but used by any of those listed in “Who this policy applies to” in accordance with the Bring Your Own Device Policy

Roles and Responsibilities

We have a responsibility to ensure that our records are managed well.

Different staff have different roles in relation to records management and these responsibilities are detailed below:

Headteacher	Overall accountability for records management and is responsible for ensuring compliance with legislation, regulation and guidance
Office Manager and Finance & Facilities Officer	Provide support to the information process owners and act as a departmental point of contact for all records management matters. Overall responsibility for managing records management risks and for ensuring effective systems and processes are in place to deliver the information security agenda
Senior Leadership Team	Pro-actively promote records management awareness and mentor and train departmental staff in records management
Information Process Owners	Are responsible for ensuring that they comply with the records management policy and standards.
Governing Board	Responsible for agreeing on the records management policy and considering and approving changes to it, along with reviewing annual reports on records management matters.
All staff, contractors, consultants and third parties	Everyone who receives, creates, maintains or has access to our documents and records is responsible for ensuring that they act in accordance with our records management policy, standards guidance and procedures.
Data Protection Officer	Responsible for assisting in monitoring compliance with this policy Responsible for advising staff on compliance with the procedures supporting this policy Responsible for assisting in the production of Privacy Impact Assessments

Retention Schedules

Data will be retained only as long as it is needed, after which it will be:

- Securely destroyed
- Anonymised
- Retained for historical or archival purposes
- Retained due to a valid business reason (e.g. for use in litigation, or in defence of a civil claim).

Documents may include personal and non-personal data. This policy applies to all data, not just personal data.

Data that is not held within a filing system (disposable data) should be securely destroyed once it no longer has a business use. This includes notebooks and diaries which should not be kept by individuals beyond their required business use.

If there is an omission in the Record Retention Schedule, or if you are unsure, please contact a senior member of staff or the Data Protection Officer.

Records (physical and electronic) that are relevant to current or potential legal proceedings, statutory investigation, audit, or any other relevant circumstances (including subject access requests), must not be deleted, disposed of, destroyed, or changed until determined those records are no longer needed.

Contact the Data Protection Officer if you are aware of contraventions of this policy or have any questions regarding retention schedules

Data storage, backup and destruction

All data must be stored in a manner that is safe, secure, accurate and accessible.

Records that are essential to business operations should have a backup and recovery strategy documented in a Business Continuity Plan.

Information Process Owners are responsible for ensuring that data has met its required retention period and ensuring its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by a secure process such as shredding. Where shredding bags are used, they must be kept securely at all times until collected by authorised personnel and destroyed.

Non-confidential data may be destroyed by recycling.

The destruction of electronic data must be coordinated with the IT Department and where appropriate a certificate of destruction is obtained when the hardware is destroyed.

Data destruction must stop immediately where records (physical and electronic) are relevant to current or potential legal proceedings, statutory investigation, audit, or any other relevant circumstances. Data destruction should commence immediately when the embargo is no longer in place.

Information Process owners are responsible for ensuring that records under their control are kept up-to-date and accurate and should take measures to ensure record validity at regular intervals.

Other relevant policies

11.1 This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- Data Protection Policy
- Acceptable Use Policy