Data Records Management Policy

December 2025

Data Records Management & Retention Policy

This policy provides the framework the school/trust will follow to achieve effective management and audit of records.

The role of records management

The school recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school/trust and provide evidence for demonstrating performance and accountability.

Our approach and commitment to records management

The school undertakes to manage records in relation to the three principles of value, integrity and accountability laid out in the Lord Chancellor's Code of Practice issued under Section 46 of the Freedom of Information Act 2000, published in July 2021.

Related policies and documents

- Retention schedule
- Data Protection policy
- Freedom of Information policy
- Data breach process
- Third party request for data process
- Other related legislation and regulations such as equal opportunities and ethics which apply to the school/trust

Roles and responsibilities

The Governing Body will:

- Establish and maintain a positive records management culture.
- Ensure the Headteacher/GDPR Officer prepares a Records Management policy for approval and adoption by the governing body and to review and monitor the effectiveness of the policy.
- Allocate sufficient resources for records management, e.g. in respect of training for staff.

- Monitor and review records management issues.
- Ensure that the school provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their responsibilities.

The Headteacher will:

- Promote a positive records management culture.
- Prepare a Records Management policy for approval by the governing body, revise as necessary and review every two years.
- Ensure that all staff co-operate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to undertake the tasks required of them.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.

The GDPR Officer will;

- Provide guidance to staff on good records management practice.
- Promote compliance with this policy so that information can be retrieved easily, appropriately and in a timely way.
- Check that records are stored securely and can be accessed appropriately at least annually.

Staff at the school will:

- Familiarise themselves and comply with the Records Management policy.
- Properly document their actions and decisions.
- Hold personal information securely.
- Only share personal information appropriately and will not disclose it to any unauthorised third party.
- Dispose of records securely in accordance with the school's/trust's Retention Schedule.

What constitutes a record?

A record is any document created, received or maintained by permanent and temporary staff of the school in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the school.

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 or activities. These records may be created, received or maintained in hard copy or electronic format.

Storage of records: digital data

Back Up System: The school will undertake regular back-ups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Backups are taken daily for the Capita curriculum server mps-004 and the sims virtual server mps-sr13. Also, daily backups for the new virtual servers maycurrsvr21-maydhcp-maywsus. All of these are backed up externally to LGFL Gridstore, which is offsite, encrypted and stored in UK based centres.

Shared Google Drives are backed up daily to LGFL Gridstore – these backups are taken between Google and Gridstore and not via the school's systems. No Gmail data is backed up, only data stored in Shared Google Drives.

Office 365 data is only backed up for the school's Head, Deputy Head and School Business Manager.

Controlling the Storage of Digital Data: Personal information is not to be stored on the hard drive of any laptop or PC unless the device is running encryption software (Bitlocker is currently being activated on children's and teacher's laptops).

The school's Bring Your Own Device policy outlines how data can be accessed and stored on personal devices.

Password Control: The school will ensure that data is subject to a robust password protection regime, three random words have been suggested to set as passwords. Password sharing is not encouraged. Staff are required to lock their PCs when they are away from their desks to prevent unauthorised use.

Location of Server Equipment: The school will ensure that the server environment is managed to prevent access by unauthorised people. The servers are all located in the lockable cupboard inside the Head Teacher's lockable office.

Storage of records: emails

Email accounts are not designed to be a records storage system, and therefore emails should not be retained indefinitely. Where an email contains a message or attachment which relates to a pupil, member of staff or contains information that needs to be retained for future reference, the school requires that this is moved from the individual's email account to the relevant area within the official hard copy or digital data storage system. This content will then fall within the relevant section of the school's Retention Schedule.

Where emails do not contain information that needs to be retained, they should be deleted at the earliest opportunity and by no later than 3 years and in line with the process outlined within the 'Disposal of Records' section of this policy.

Storage of records: hard copy data

Storage of Physical Records: The school recommends that all physical records are stored in filing cabinets, drawers or cupboards. Sensitive physical records should be kept in a lockable storage area. This is to prevent unauthorised access but also to protect against the risk of fire and flooding.

Unauthorised Access, Theft or Loss: Staff are encouraged not to take personal data on staff or students out of the school unless there is no alternative. Records held within the school should be in lockable cabinets.

Clear Desk Policy: In order to avoid unauthorised access to physical records which contain sensitive or personal information and to protect physical records from fire and/or flood damage, the school operates a clear desk policy. This involves the removal of the physical records to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all contents.

Retention of records

The school has documented how long it will retain specific records within its Retention Schedule. This schedule contains recommended retention periods for the different records created and maintained by educational settings in the course of their business. The schedule refers to all information regardless of the media in which it is stored.

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of data protection legislation.

Managing records using these retention guidelines will be deemed to be 'normal processing' under data protection legislation. If records are to be kept for longer or shorter periods than laid out in the schedule then the reasons for this need to be documented.

Disposal of records

Records should not be kept for any longer than is necessary in relation to the purpose for which they were originally collected/processed. The Retention Schedule sets out the retention periods for all records held by the school.

All records containing personal information or sensitive policy information should be made either unreadable or unreconstructable.

- Physical records should be shredded.
- Electronic records should be deleted.
- Emails should be deleted.
- Hardware containing personal information should be destroyed.

If an external company is used for any part of the disposal process, the company must provide a Certificate of Destruction to evidence secure disposal of the record.

Monitoring compliance

The GDPR Officer will check that records are stored securely, in line with the retention schedule and that they can be accessed appropriately at least annually and provide a report for the Headteacher and Governing Body.

Other

In the event of an incident involving the loss of information or records held by the school, the Data Breach process should be followed.

If the school receives a request for information from a third party, then the process outlined in the Third Party Requests for Information process should be followed.