



Records Management Policy

1.0 Introduction

Pond Meadow recognises the necessity for the efficient management of its records to comply with its legal and regulatory obligations and to contribute to the effective overall management of the school.

2.0 Scope of the Policy

This policy applies to all records created, received or maintained by the staff in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business of the school and which are therefore 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 electronically.

A small percentage of the school's records may be selected for permanent preservation as part of the school's archives and for historical research.

3.0 Responsibilities

The school has a responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The Headteacher has overall responsibility for this policy.

The Office Manager is responsible for staff, payroll, and pupil records and the Finance Officer for financial records. The relevant responsible person will give guidance on good practice and promote compliance with this policy so that information can be retrieved easily, appropriately, and in a timely way.

Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the school's records management guidelines.

4.0 Recording Systems

Information created by the school must be managed against the same standards regardless of the media in which it is stored.

- 4.1** Filing of information must be carried out on a regular basis. It is equally important that extraneous information is removed on a regular basis. Removing information from a file once a Freedom of Information request has been received is a criminal offence.



4.2 Once a file has been closed it should be moved out of current filing and stored in an archive until it has reached the end of the retention period.

5.0 Information Security

Information security is very important, especially when dealing with personal or sensitive information.

5.1 All personal information must be kept in lockable filing cabinets, which are locked when unattended.

5.2 Personal information held on computer systems should be adequately password protected. Information should never be left on the screen if the computer is unattended.

5.3 Files containing personal or sensitive information should not be left out on desks overnight

5.4 Sensitive personal information should not be sent by email unless encrypted or password protected.

5.5 If files are taken off the premises they should be left secured.

5.6 Files must not be carried using a memory stick or other removable data

5.7 All computer based information should be backed up regularly and the back up stored off site.

5.8 Information contained in emails should be filed into the appropriate electronic or manual filing system once it has been dealt with.

6.0 Safe Disposal of Information

Information should be disposed of in accordance with the guidelines for schools by the Information and Records Management Society (IRMS). A copy of which is kept in the Finance office or online at www.irms.org.uk. This process should be undertaken on an annual basis during August.

All personal information should be disposed of in the red Deadman Confidential bin.

Electronic data should be archived on electronic media and deleted appropriately at the end of the retention period.

7.0 Relationship with existing policies

The policy should be read in conjunction with other relevant legislation and regulations and the following school policies:

- Data Protection Policy
- Freedom of Information Policy