Naphill and Walters Ash Schools Record Management Policy

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, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

It covers:

• Scope

• Responsibilities

• Relationships with existing policies

1. Scope of the policy

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

1.2 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 electronically.

1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service

2. Legal Framework

This policy has due regard to legislation including, but not limited to;

1. General Data Protection Regulation 2016
2. Freedom of Information Act 2000
3. Limitation Act 1980

This policy will be implemented in accordance with the following school policies and procedures;

1. Freedom of Information
2. Data Protection Policy
3. Security Breach Management Plan
4. And with other legislation and regulations (including audit, equal opportunities and ethics) affecting the school.

3. Responsibilities

3.1 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 Head of the School.

3.2 The Data Protection Officer (DPO) is responsible for the management of the records at Naphill and Walters Ash School.

3.3 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. They will also monitor compliance with this policy by surveying at least annually, in conjunction with the Head, to check if records are stored securely and can be accessed appropriately.

3.4 The DPO is responsible for ensuring that all records are stored securely, in accordance with retention periods as set out in Retention Schedule, and are disposed of correctly.

3.5 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 record management guidelines.

4.Storing and Protecting Information

Information created by the school must be managed against the same standards regardless of the media in which it is stored. The DPO will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.

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

4.1 It is important that filing information is properly resourced and is carried out on a regular basis. It is equally important that the files are weeded of extraneous information where appropriate on a regular basis. Removing information from a file once a freedom of information request has been made will be a criminal offence (unless it is part of normal processing).

4.2 Applying retention periods is straightforward provided files are closed on a regular basis.

4.3 Once a file has been closed, it should be moved out of the current filing system and stored either in a record room in the school or in another appropriate place until it has reached the end of the retention period.

4.4 All personal information and confidential records should be kept in lockable filing cabinets or drawers which are kept locked when the room is unattended. Access to these should be restricted.

4.5 Confidential paper records are not left unattended or in clear view when held in a location with general access.

4.6 Files containing personal or sensitive information should not be left out on desks overnight, there should be a 'clear desk' policy.

4.7 If personal information/data has to be taken off the premises it should be secured in the boot of a car or in lockable containers. The person taking the information from the school premises accepts full responsibility for the security of the data.

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

4.9 Where data is saved on removable storage or portable device, the device is kept in a locked and fireproof cabinet or drawer when not in use. E.g. school keeping records on such devices.

4.10 Teachers should not use USB sticks or external hard drives to store personal data on for use at home unless device is password protected and fully encrypted.

4.11 All devices that staff use to access personal data must be password protected.

4.12 Staff do not use personal devices for school purposes.

4.13 All staff should have secure login and password which are not shared.

4.14 Emails containing sensitive or confidential information are password protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

4.15 if sending confidential information by fax, staff will check that the recipient is correct before sending.

4.16 Circular emails to parents are sent blind carbon copy (BCC) so email addresses are not disclosed to other recipients.

4.17 Information contained in email, fax should be filed into the appropriate electronic or manual filing system once it has been dealt with. (see email use guidance)

4.18 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing personal information will be supervised at all times.

4.19 The physical security of the school buildings and storage systems, and access to them, is reviewed termly by the site manager and DPO. If an increased risk of vandalism, burglary or theft is identified, this will be reported to the head and extra measures to secure data storage will be put in place.

4.20 The school takes its duties under GDPR seriously and any unauthorised disclosures may results in disciplinary action.

4.21 The DPO is responsible for continuity and recovery measures being in place to ensure the security of protected data.

4.22 Any damage or theft of data will be managed in accordance with the school's Security Breach Management Plan.

5 The Safe Disposal of Data

5.1 Files should be disposed of in line with the attached retention schedule (see appendix). This is a process which should be undertaken on an annual basis.

5.2 Paper records containing personal information should be shredded using a cross-cutting shredder. Other files can be bundled up and put in a skip or disposed of to the waste paper merchant. Loose papers should not be put in skips unless the skip has a lid. CD's/DVD's/Floppy disks should be cut into pieces. Audio/Video tapes and fax rolls should be dismantled and shredded.

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

5.4 The DPO will keep a record of all files that have been destroyed.

5.5 Where the disposal action is reviewed before disposal the DPO will review the information against its administrative value. If it has value the DPO will keep a record of this. The DPO will review the information after three years and conduct the same process.

5.6 If reviewed and the data is deemed for disposal it will be destroyed in accordance with the disposal action listed on the Retention schedule.

6 Monitoring and Review

This policy has been reviewed and approved by the head teacher and governors. The Records Management Policy will be reviewed and updated as necessary every 2 years.