Data Records Management & Retention Policy

January 2018

sbm services
school business management

Contents

Data Records Management & Retention 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.

1: Scope of the Policy

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

Records are defined as all those documents that 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.

2: 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 Data Protection Officer.

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.

The Data Protection Officer will monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

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 retention guidelines.

3: Information Security & Business Continuity

In order to protect the data and records the school is responsible for, the following security measures will be implemented.

The Storage & Security of 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.

Offsite backup using Computer Talk Azure – Europe (Mirrors local backup)

Offsite backup using ECC Attix 5 – Europe. Daily backup). This is limited in size (for critical files) which includes SIMS, FMS and a selection of files in the Admin Shared area, Finance area, Office Manager personal account and Head Teacher personal account.

Local & Azure Offsite Backup retentions

Server name	Type	Duration	retention period
BTBJ-FIL-001	User and shared areas	Daily	25 days
BTBJ-MIS-001	SIMS backup	Daily	5 days
BTBJ-APP-001	VM Backup	Weekly	5 days
BTBJ-FIL-001	VM Backup	Weekly	5 days
BTBJ-MIS-001	VM Backup	Weekly	5 days
BTBJ-SRV-001	VM Backup	Weekly	5 days

The school tests that data can be restored from a back up on a termly basis by choosing a random file. Checking of the backup logs are made weekly to ensure a successful backup has taken place.

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.

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 <Minimum of 8 Characters and must include at least one capital letter, lower case letter and a number >. 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 main school server is located in the IT Suite, hidden away from windows under the desk. The backup server is located as far away from the main server as possible in the SBM office, hidden away from windows under desks. Each has its own UPS>

The Storage & Security of 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 will 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.

4: Disclosure / Confidentiality

Staff are made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it and that consideration has been given to the General Data Protection Regulations. This is outlined in the Staff Handbook.

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.

5. Safe Disposal of Records

The General Data Protection Regulations give individuals the Right to Erasure which means that records should not be kept for any longer than is necessary in relation to the purpose for which it was originally collected/processed (see section 6 Retention Guidelines).

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

- Paper records should be shredded using a cross-cutting shredder
- CDs/DVDs/Floppy Discs should be cut into pieces
- Audio/Video Tapes and Fax Rolls should be dismantled and shredded
- Hard discs should be dismantled and sanded

Where an external provider is used, the disposal company must provide a Certificate of Destruction.

6. Security Breach

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

7: Retention Guidelines

This retention schedule contains recommended retention periods for the different records created and maintained by schools 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 the Data Protection Act (DPA).

Managing record series using these retention guidelines will be deemed to be 'normal processing' under the legislation mentioned above. If records are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

Policy Date: Spring Term 2018

Review Date: Spring Term 2019