Beaucroft Foundation School

Data Retention and Records Management Policy

Beaucroft Foundation 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:

1. Scope
2. Responsibilities
3. Relationships with existing policies
4. The purpose of the retention policy
5. Benefits of a retention schedule
6. Recording systems
7. What to do with records once they have reached the end of their administrative life.
8. Monitoring and Review

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. Also, by any agents, contractors, consultants or third parties acting on behalf of the school.

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.

2. Responsibilities

2.1 The school has a statutory responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The persons with overall responsibility for this policy are the Co-Headteachers.

2.2 The school's Data Protection Lead 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 to check if records are stored securely and can be accessed appropriately.

2.3 The school will manage and document its records disposal process in line with the Records Retention Schedule. This will help to ensure that it can meet Freedom of Information requests and respond to requests to access personal data under data protection legislation (subject access requests "SARS").

2.4 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. The guidelines stipulate that they:

2.4.1 Manage the school's records consistently in accordance with the school's policies and procedures;

2.4.2 Properly document their actions and decisions;

2.4.3 Hold personal information securely;

2.4.4 Only share personal information appropriately and do not disclose it to any unauthorised third party;

2.4.5 Dispose of records securely in accordance with the school's Retention Schedule.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- Subject Access Request policy
- Data Protection policy
- Data Retention schedule
- and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

4. The purpose of the Retention Policy

The retention policy stipulates the length of time a record needs to be retained and the action which should be taken when it is of no further administrative use. Members of staff are expected to manage their current record keeping systems using the retention schedule, and to take account of the different kinds of retention periods when creating new recording

systems. The retention schedule refers to all information, regardless of the media in which they are stored.

5. Benefits of a retention schedule

There are a number of benefits which arise from the use of a complete retention schedule:

- Managing records against the Retention Policy is deemed to be “normal processing” under the GDPR (2018) and the Freedom of Information Act 2000. Provided members of staff are managing record series using the Retention Policy they cannot be found guilty of unauthorised tampering with files once a freedom of information request or a subject access request (SAR) has been made.
- Members of staff can be confident about destroying information at the appropriate time and in a secure manner.
- Information which is subject to Freedom of Information and GDPR legislation will be available when required.
- The school is not maintaining and storing information unnecessarily.

6. Recording Systems

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

6.1 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).

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

6.3 Once a file has been closed, it should be moved out of the current filing system and stored either in a locked room in the school until it has reached the end of the retention period.

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

6.5 Information security is very important especially when dealing with personal information or sensitive policy information. There are a number of basic rules: ·

- All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended.
- 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.
- Files containing personal or sensitive information should not be left out on desks overnight.
- Where possible sensitive personal information should not be sent by e-mail.
- If files need to be taken off the premises they should be secured in the boot of a car or in lockable containers.

- Teachers have been advised not to use data on memory sticks or other removable data carriers in order to access their files both at home and at school. Instead they should use the remote access.
- All computer information should be backed up regularly and the back-up should be stored off the site.

7. What to do with records once they have reached the end of their administrative life.

7.1 Destruction of records
Where records have been identified for destruction, they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information should be shredded before disposal.

7.2 Transfer of records to the Archives
Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Archives.

7.3 Transfer of information to other media
Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

8. Monitoring and Review

This policy will be reviewed on an annual basis by the school's Data Protection Officer alongside all other documents and policies relating to data protection. Any suggestions for amendments will be presented to the governors for their approval following review.