THE HEATH ACADEMY TRUST

DATA RECORD MANAGEMENT & RETENTION POLICY

inspire transform together

Summary	
Policy Reference Number:	025
Category:	Data Protection
Authorised By:	Board Of Directors
Committee Responsible:	Board Of Directors
Version:	2018-1
Status:	21/03/2018: Approved at Full Trust Board.
Next Review Date:	21/03/2019

Registration Number: 09809895

Contents

Definitions
Note: These terms are standard throughout all policy documents and are designed to provide clarity.

Section 1: The MAT

"the Academy Trust" *and* "Trust"	mean the Heath Academy Trust Company.
"the Board"	means the Board of Directors of the Heath Academy Trust Company.
"the Directors"	refers to the group of (up to 12) Directors who make up the Board, and who are also the Heath Academy Trust's "Trustees" under charity law.
"Finance Committee"	refers to the Finance and Audit Committee formed by the Board to manage the financial affairs of the Trust.
"Accounting Officer"	is a role held by the Chief Executive Officer ("CEO") of the Trust, and one which includes a personal responsibility for the financial resources under the Trust's control. He is accountable for the Trust's financial affairs.
"Chief Finance Officer" (CFO)	is the Trust's finance director, and also the Trust Business Manager, to whom the Accounting Officer delegates responsibility for delivery of the Trust's financial processes and reports , and for the oversight and consolidation of the Academies' financial data.
"Trust Business Manager" ("TBM")	Fulfils the CFO role within the Trust, including compliance and statutory returns, as described in the Academies' Financial Handbook.
"Leadership Team"	is a team representing the Academies, consisting of the Headteachers and the CEO, and the TBM.

A full description of the positions listed and their responsibilities will be found in the current Academies' Financial Handbook.

Section 2: The Schools

"Academy"	One of the six schools making up the Heath Academy Trust.
"Academies"	All of the six Academies.
"School"	means an Academy within the Trust.
"Finance Officer"	The person responsible for the day to day management of an Academy's financial operations.
"Governor"	means a formally elected and appointed member of a School's Governing Body (generally referred to as the LGB).
"Headteacher"	means the senior person at an Academy who may also be an Executive Headteacher and/or elected as a Director of the Board.
"School's Leadership Team"	A group within each School consisting of the Headteacher, senior staff and the local Governing Body.

1. Introduction

1.1 The Heath Academy Trust 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.

1.2 Scope Of The Policy

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

1.2.2 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

2.1 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 Trust Board.

2.2 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.

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

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 retention guidelines.

3. Information Security & Business Continuity

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

3.2 The Storage & Security Of Digital Data

3.2.1 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. Back up are undertaken by Academy IT

3.2.2 The school tests that data can be restored from a back-up on a regular basis.

3.3 Controlling The Storage Of Digital Data

3.3.1 Personal information is not to be stored on the hard drive of any laptop or PC unless the device is running encryption software.

3.3.2 The Trust Bring Your Own Device Policy outlines how data can be accessed and stored on personal devices.

3.4 Password Control

3.4.1 The school will ensure that data is subject to a robust password protection regime. Academy IT issue all staff with passwords.. Password sharing is not encouraged. Staff are required to lock their PCs and any other devices when they are away from their desks to prevent unauthorised use.

3.4.2 Location Of Server Equipment

The school will ensure that the server environment is managed to prevent access by unauthorised people. The server is located in a locked cabinet. The server is monitored by Academy IT.

3.5 The Storage & Security of Hard Copy Data

3.5.1 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.

3.5.2 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.

3.5.3 Clear Desk Policy

In order to avoid unauthorised access to physical records which contain sensitive or personal information, 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

4.1 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.

4.2 If the school receives a request for information from a third party, then the process outlined in the 3rd Party Request For Information Process should be followed.

5. Safe Disposal Of Records

5.1 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 7 on Retention Guidelines).

5.2 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
- if an external provider is used all records must be shredded on site in the presence of an employee. The disposal company must provide a Certificate of Destruction.

6. Security Breach

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

7. Retention Guidelines

7.1 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.

7.2 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).

7.3 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. The schedule should be reviewed on an annual basis.