THE HEATH ACADEMY TRUST

DATA BREACH PROCEDURE

inspire transform together

Summary	
Policy Reference Number:	n/a
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

The Heath Academy Trust
Registered Address: St Ives Primary & Nursery School, Sandy Lane, St. Ives, Ringwood, Hampshire, BH24 2LE
Registered in England and Wales
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 Although the Heath Academy Trust and all its schools take measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this procedure and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the deceiving the Heath Academy Trust and its schools.

1.2 However the breach has occurred, the following steps should be taken immediately:

1. Internal Notification: Individual who has identified the breach has occurred must notify the School Data Protection Officer/Data Protection Controller. A record of the breach should be created using the following templates:

- Data Breach Incident Form (Appendix A)
- Data Breach Log (Appendix B)
- Data Breach Evidence Log (Appendix C)

2. Containment: Data Protection Officer/Data Protection Controller to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. Recovery: Data Protection Officer/Data Protection Controller to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. Assess the risks: Before deciding on the next course of action, Data Protection Officer/Data Protection Controller to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form (Appendix A):

a. What type of data is involved
b. How sensitive is it?
c. If data has been lost/stolen, are there any protections in place such as encryption?
d. What has happened to the data?
e. What could the data tell a third party about the individual?
f. How many individual's data have been affected by the breach?
g. Whose data has been breached?
h. What harm can come to those individuals?
i. Are there wider consequences to consider such as reputational loss?

5. Following the risk assessment in step 4 the Data Protection Officer/Data Protection Controller should contact the Data Protection Officer/Data Protection Controller at their paired school and discuss the evidence in the Data Breach Notification form (Appendix A). The Trust Data Protection Officers may also be contacted if further support is felt necessary.

6. Notification to the Information Commissioners Office (ICO): Following an independent review of the evidence the Data Protection Officer/Data Protection Controller from the paired school will, if appropriate, notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

The Data Protection Officer/Data Protection Controller from the paired school should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

7. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the School

8. **Evaluation:** The Data Protection Officer/Data Protection Controller from the paired school should assess whether any changes need to be made to the School processes and procedures to ensure that a similar breach does not occur.

Appendix A

Data Breach Incident Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	

Whose data has been breached:	
What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss:	

Part C: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	