DATA BREACH POLICY AND PROCEDURE DECEMBER 2020

Approved Trust Board:
02 December 2020
Version 1.0
Review: Every 3 years

Esteem Multi-Academy Trust

Data Breach Policy and Procedure

Introduction

The Esteem Multi-Academy Trust (EMAT) is committed to protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018. The Act brought the EU's General Data Protection Regulation (GDPR) into UK law. The Trust gathers and processes personal information about its staff, students, and other individuals to comply with obligations as a charitable company limited by guarantee that is responsible for academies.

To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. All academies within the trust process personal information about staff, pupils, parents and other individuals who come into contact with each academy as part of the usual day to day business of a school. It is important that all staff, local governors and trustees are aware of what to do in the event of a Data Protection Act (DPA) / General Data Protection Regulations (GDPR) breach. The following guidance sets out the correct procedures to follow, required actions to take and provides the documentation to complete in such an event.

What's Considered a Data Breach?

The term 'data breach' is often used synonymously with cyber-attacks. However, not all cyber-attacks result in data breaches, and not all data breaches are the result of a cyber-attack. A data breach is whenever the confidentiality, integrity and availability of information is compromised. Data doesn't only need to be stolen to be breached; it might also have been lost, altered, corrupted or accidentally disclosed.

Data breaches can happen to any kind of information, but the GDPR is concerned only with personal data. Any breach of the Data Protection Act 2018 or the General Data Protection Regulations may be considered to be an offence, and in that event relevant disciplinary procedures will apply.

The GDPR: What exactly is personal data?

Personal data is at the heart of the GDPR (General Data Protection Regulation). There is no definitive list of what is or isn't personal data, so it all comes down to properly interpreting the GDPR's definition:

'[P]ersonal data' means any information relating to an identified or identifiable natural person ('data subject').'

In other words, any information that is clearly about a particular person. But just how broadly does this apply? The GDPR clarifies:

'[A]n identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

Breaches

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported and appropriate prompt action is taken, they are often manageable.

Examples of personal data breaches in schools

- **Unauthorised access**: A pupil or unauthorised staff member finds a teacher's laptop unlocked and uses it to access saved files. The teacher might also have autosaved login details for their email or other accounts, which would give the user access to further information.
- **Deliberate or accidental action (or inaction)**: A member of staff sends an old PC to be destroyed without wiping the hard drive. Another example is physical records that are thrown away without first being shredded.
- **Accidental disclosure**: An administrator sends an email containing a student's personal data to the wrong recipient.
- **Alteration**: Someone accesses the school's payroll system and enters incorrect information about staff pay grades.
- **Loss of availability**: The school suffers a power cut that shuts down access to information that's only available electronically.

Reporting – When should a breach be reported?

The GDPR states that personal data breaches must be reported if they pose a risk to the rights and freedoms of those affected. This will be the case if the breach is likely to result in:

1. **Discrimination**
   This is relevant when the following information is breached:
- Pupil special needs information
- Staff and pupil health records
- Child protection records
- Staff pay scale and payroll information
- Pupil progress and attainment records

2. **Identity theft or fraud**
   This is relevant when the following information is breached:
- Names, dates of birth and addresses (when breached together)
- Completed pupil data collection sheets

3. **Financial loss**
   This is relevant when the following information is breached:
- Banking information from payroll data or recruitment forms
- School parent payment software, billing information or bank accounts

4. **Reputational damage**
   This is relevant when the following information is breached:
- Staff performance management records
- Pupil behaviour records
- Child protection records

5. **Loss of confidentiality**
   This is relevant when the following information is breached:
- Staff performance management records
- Child protection records

6. **Social disadvantage**
   This is relevant when the following information is breached:
- Payroll information
- Pupil premium records
- Information about pupils receiving bursary or other financial support

7. **Sensitive information**
   Breaches must also be reported whenever **sensitive information** is affected:
- Racial or ethnic origin
- Political opinions, religion or philosophical beliefs
- Trade union membership
- Genetic data
- Health data
- Data concerning sex life
- Criminal convictions and offences or related security measures

Breach / Potential Breach - What should you consider?

In the event of a breach (or a potential breach if you are unsure whether the matter presented constitutes a breach) the 'Data Breach Flowchart' outlines the process that should be followed and should be considered alongside this policy (**see annex 1**).

The 'Data Breach Form' must be completed and updated as the process progresses (**see annex 2**)

What Should You do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the Information Commissioners Office (ICO) and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Each of the academies within our trust has an appointed lead for data protection. This is usually the School Business Manager and/or GDPR lead. All breaches must be immediately reported to the appointed academy lead and they are responsible for completing the breach notification form and maintaining a breach register. The academy lead will report the breach/possible breach to the Data Protection Officer (DPO) immediately and ensure that the EMAT Governance Officer is copied into any correspondence on this matter. This is essential.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, notification to those people will be done in a coordinated manner with support from the DPO.

A breach report will be made by the DPO within 72 hours of becoming aware of the breach.

It may be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification

For every breach the academy (with guidance from the DPO) must consider notification to the data subject or subjects. If the breach is likely to be considered high risk they will be notified as soon as possible and will be kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and records containing personal data , the most effective notification will be used and discussed with the Data Controller (Trust) with support from the DPO. Advice may also be taken from the ICO about how to manage communications with data subjects.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data has occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings). This may also be used as a source of information for the ICO, and it could also be used within criminal or civil proceedings.

This process will be conducted by the academy's GDPR lead, the governance officer or the DPO dependent upon the nature of the breach.

Advice may be required from external legal providers and the police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored, and secured must be available as a separate log (please see example below). Files and hardware must be securely stored and the DPO may advise on this.

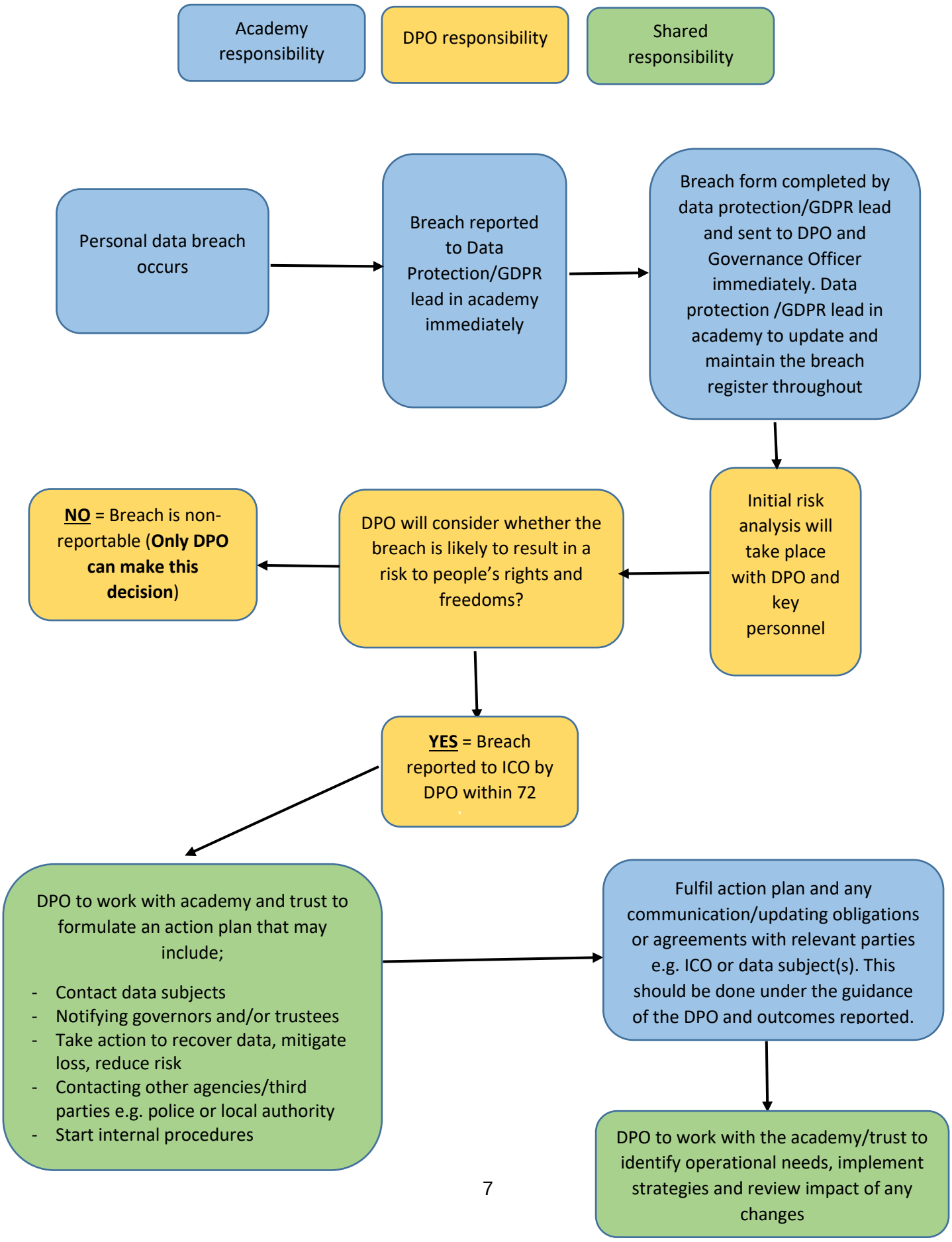
Example evidence storage record;

DPO name: **Data Breach Reference:** **Academy Name / Central Team:** **GDPR Lead / Academy Lead:**			
Data Breach Evidence Log			
Date	Evidence Description	Secure storage location and date added to name of file	Name of person who gathered the evidence

Post Breach Action

It is important that a post breach action plan is put into place and reviewed.

Annex 1 EMAT Breach Management Flowchart



Annex 2 EMAT Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in the school?	
Who was this reported to?	
Date and time it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers	
The categories of personal data affected –electronic, hard copy	
Approximate number of data subjects affected.	
Approximate number of personal data records affected.	
Name and contact details of the Data Protection Officer and GDPR Lead.	
Consequences of the breach. What are the potential risks?	
Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	