Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

Data Breach Policy

Approved by Trust Board on 13 July 2018
Applicable from 1 September 2018

1.0 Purpose

The Co-operative Academies Trust (the Trust) and its academies are required to follow the General Data Protection Regulation (GDPR) in the way that it collects and uses personal data. Section 2 of Chapter IV of the GDPR sets out the requirements for data controllers to implement appropriate security measures and how personal data breaches should be notified.

This policy sets out the approach that will be taken by the Trust's central team and its academies to deal with personal data breaches.

This policy applies to:

- All employees of the Trust whether based in an academy or in the Trust's central team
- Trust Board members and governors and

2.0 Introduction

The GDPR describes the responsibilities that organisations have when dealing with personal data. Personal data is defined as any information relating to an identified or identifiable natural person. The person is known as a 'data subject'.

The sixth principle of data protection states that personal data shall be *'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.'*

Notwithstanding these measures it is inevitable that sometimes this principle will be broken, creating a personal data breach. Three types of breaches can occur:

- Confidentiality – unauthorised access or use of personal data
- Availability – personal data that should be available is not accessible
- Integrity – inaccurate personal data has been recorded

In the event of a data breach being discovered there are a set of key actions which must be undertaken. These steps are likely to require action from academy based staff and staff based in the Trust's central team.

3.0 Related Policies

This policy is closely linked with other Trust and Academy policies which should referenced when appropriate, including:

- Data protection
- Staff Code of Conduct, including Electronic Communications
- Any other relevant guidance documents

4.0 Responsibilities

Trust's academies and their governing bodies will:

- Put in place a clear procedure for dealing with personal data breaches. This procedure should take account of the requirements laid down in Annex X.
- Follow any additional guidance from Trust or the Information Commissioner's Office (ICO) produced subsequently to this policy
- Inform the Trust's Data Protection Officer of all personal data breaches
- Record the details of personal data breaches made in the system provided by the Trust for this purpose
- Ensure that personal data breaches are dealt with in line with the statutory time limits and notify the Trust's Data Protection Officer as soon as possible if these limits can't be met
- Take advice from the Trust's Data Protection Officer with regards to the management of personal data breaches

The Trust will:

- Provide guidance and support to any academy dealing with a personal data breach
- Provide a route of communication to the ICO in the event of notification being required and any follow-up actions

5.0 Review

The Trust's policy on Data Subject requests will be reviewed annually, or when the (ICO) issues revised guidance on this topic.

Annex 1

Requirements of the procedure for managing personal data breaches

1. Data Breach Teams

Potential or actual data breaches either in the Trust or within one of the Trust's academies, pose the greatest threat in terms of financial penalty to the Trust Board, and reputation to the Co-op Group. That being the case, their management and mitigation needs to handled by senior staff within the Trust and its academies and by staff who are able, without restriction to bring about immediate mitigation of a potential or actual breach.

In order to manage potential data breaches, the Trust and its academies require the permanent formation of a Data Breach Team which comes together on internal notification of a potential breach.

The Data Breach Team for the central trust team will manage the response to potential and actual breaches relating to data processed by its central teams.

This Data Breach Team will be managed by the Trust's Data Protection Officer (DPO) and will additionally comprise a senior representative of each area of the central team's functions. The Trust's Data Breach Team (for its central teams) therefore comprises:

- The Data Protection Officer (and Governance Manager)
- The Trust's Director
- The Finance and Resources Director (and cover DPO in the absence of the DPO)
- The Education Director, East Pennines
- The Education Director, West Pennines
- The Head of Human Resources

Each academy will have its own data breach team which will manage the response to potential and actual breaches relating to data processed by their academy. The membership of these teams will reflect the membership of the Data Breach Team for the Trust's central team, including the GDPR Ambassador. The Trust's DPO (or cover DPO) should be informed immediately of a potential or actual breach and will oversee and have final sign off of actions to be taken and before any contact is made with the ICO.

2. Procedure overview

The procedure for managing personal data breaches needs to be implemented in detail by the Data Breach Team in the Trust's central and academy based teams. These procedures need to take account of the following stages and requirements.

i. Discovery of a personal data breach
ii. Investigate the nature of the breach
iii. Take action to contain the breach
iv. Assess the level of notification required
v. Notify appropriate parties
vi. Identify actions to minimise the reoccurrence of the breach

3. Discovery of a personal data breach

Any member of staff in the central team or at one of the academies may identify that a breach has occurred. They may also receive a report from a student or any other stakeholder that a potential breach has occurred.

It is essential that when a breach is discovered that it is reported as soon as possible.Understanding of the chronology of the event is important to properly assess the risk it poses. In addition, actions can be taken to contain the impact of breach provided they can be taken quickly enough.

Reporting breach makes a positive contribution to managing the Trust's and academies' data protection responsibilities.

It should be noted that at the point any member of staff becomes aware of a breach this is the start of the 72 hour clock for response; this is not when the GDPR Ambassador or the DPO is informed. For example if a member of staff's car is broken into on Friday evening and a laptop is stolen – this is the discovery of the breach and not when it is reported to the academy's GDPR Ambassador after the weekend.

To make this reporting possible, communication routes need to be established which are specifically operational outside of normal office hours.

A dedicated email address and/or telephone number to receive such notifications would be suitable. Arrangements for how these lines of communications are covered should be managed locally by the central team or an academy.

4. Investigate the nature of the breach

The core focus at this stage is to have enough information to determine if notification to the ICO will be required. To make this decision the essential information is:

- The type and numbers of data subjects affected
- The types of personal data compromised and the number of records
- A general idea of the cause of the breach
- The possible consequences of the breach
- Any factors that mitigate the risk from the breached data

The decision to notify the ICO or not is based upon the scale, scope and impact of the risk. The person who discovered the breach will need to give some detail about the event. With the initial results from the investigation, a preliminary decision can be made about the level of notification required.

Where notification to the ICO is not required and once containment action is underway, the breach can be managed within the normal working week. On the other hand if notification seems likely or the decision is borderline then the investigation will need to look at the event in more detail.

5. Take action to contain the breach

This step runs largely parallel with the investigation. Containment means taking action to limit the potential consequences of the breach. This is why the Data Breach Team must have authority to act. Providing the breach has been reported quickly, significant mitigation is possible. This is likely to be about computerised systems rather than paper records.

Lost or stolen devices can be locked or wiped remotely, credentials can be forced to change and deleted records may be able to be retrieved from network backups. These methods are more likely to work if the time to put them into operation is as close to the breach event as possible.

If criminal action is suspected, then a police report should be filed at this point. If there is strong evidence that a member of staff has deliberately breached information, then a disciplinary action needs to be initiated.

Even if the actual breach event happened some time before discovery, the questions about whether actions can be taken to mitigate the further spread of breached information should be considered. It can of course be far more difficult to achieve in these circumstances.

6. Assess the level of notification required

This is a decision that must involve the GDPR Ambassador and usually will involve the Trust's Data Protection Officer as well. No simple threshold numbers can be used. Very sensitive information about a small number of people could have very significant impacts on them or other people while relatively benign data about a large number of people may have little risk to their rights and freedoms.

The rationale for the decision about reporting should be recorded and kept with other details of the breach. If a judgement Is made that the ICO must be notified, then it's likely that further investigation will be required before the report can be completed. This means that this decision about notification really needs to come well before the 72-hour window closes.

7. Notification of the breach

This task, unless there are exceptional circumstances, will be carried out by the Trust's Data Protection Officer. Part of the role is to be the interface between the data controller and the regulator. The critical requirement is for the investigation to have been completed and any potential action to contain the breach needs to be in progress or planned.

Members of the Breach Team will need to be available to answer any questions that the ICO may have and to take actions that are recommended.

If notification to the ICO is not required, then the information about the breach it recorded in the academy's own log. The same basic information that would go into the ICO notification should go into the local breach log. For local logging the 72-hour timescale is not enforced.

8. Repair the causes of the breach

It is not always possible to identify exactly where a breach has come from, but once the heat of the moment has cooled then a more patient review of the situation can identify a systemic issue. As before, it's crucial that people are not put off from reporting breaches. This repair phase should not, unless malicious action is identified, be seen as a search for someone to blame.

Ideal outcomes would be the recognition for more training, further tightening of access controls and a renewed effort for email hygiene.

In the event that a significant failing is likely then a full data protection impact assessment can help to find the breach risks and mitigate them.