Academies Trust

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

Data Breach Policy

Approved by the Trust Board on 20 October 2022

Applicable from 21 October 2022

Appendix 3 of Data Protection Policy

1. Purpose

The Co-operative Academies Trust, including all of its academies, is required to follow the Data Protection Act (2018) and the UK Data Protection Regulation (the UK GDPR) in the way that it collects and uses personal data.Section 2 of Chapter IV of the UK 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 the Trust will take to deal with personal data breaches.

This policy applies to:

- All employees the Trust whether based in an academy or in the Trust's central team
- All members of the academy local governing bodies (LGBs) or any group which replaces these, Trustees and Members of the Trust

The Trust has a centrally employed Data Protection Officer who can be contacted via data@coopacademies.co.uk.

2. Introduction

The UK 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 the measures that Data Controllers put in place, it is inevitable that sometimes a failure will occur with respect to this principle, creating a personal data breach. Three types of breaches are recognised:

- 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, there are a set of key actions which must be undertaken.

3. Related policies

This policy is closely linked with the Trust's data protection policy.

4. Responsibilities

The Trust will:

- Put in place a clear procedure for dealing with personal data breaches. This procedure is detailed in the Trust's Data Protection Handbook which is made available to all academy GDPR Ambassadors;
- Follow any additional guidance from the Information Commissioner's Office (ICO) produced subsequently to this policy;
- Inform the Data Protection Officer of all personal data breaches;
- Record the details of personal data breaches and make those records available to the Data Protection Officer;
- Ensure that personal data breaches are dealt with in line with the statutory time limits and notify the Data Protection Officer as soon as possible if these limits can't be met;
- Take advice from the Data Protection Officer with regards to the management of personal data breaches.

The Data Protection Officer will:

- Provide guidance and support in dealing with a personal data breach;
- Provide a route of communication to the Information Commissioner's Office in the event of notification being required and any follow-up actions.

5. Implementation of policy

This Policy shall be deemed effective on 22 October 2022.

6. Review

This policy on personal data breaches will be reviewed bi-annually, or when the Information Commissioner's Office (ICO) issues revised guidance on this topic.