DATA BREACH POLICY

Version:	1.0
Date created:	July 2018
Author:	C Brown
Ratified by:	Executive Team
Date ratified:	18 December 2018
Review date:	September 2020

Revision History:

Version	Date	Author	Summary of Changes:
1.0	July 2018	C Brown	New policy

1 Policy Statement

1.1 The Trust is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.2 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.3 All members of our **workforce** (in the academies, Teaching School, SCITT and central Trust team) must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 This policy informs all of our **workforce** on dealing with a suspected or identified data security breach.

2.2 In the event of a suspected or identified breach, staff in the academy/Trust must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

2.3 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

2.4 The Trust must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioner's Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

2.5 Failing to appropriately deal with and report data breaches can have serious consequences for the academy/Trust and for **data subjects** including:

2.5.1 identity fraud, financial loss, distress or physical harm;

2.5.2 reputational damage to academy/Trust; and

2.5.3 fines imposed by the ICO.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in bold text, and a list of definitions is included in Annex 2 to this policy.

4 Identifying a Data Breach

4.1 A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

4.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

4.2.1 Leaving a mobile device on a train;

4.2.2 Theft of a bag containing paper documents;

4.2.3 Destruction of the only copy of a document; and

4.2.4 Sending an email or attachment to the wrong recipient; and

4.2.5 Using an unauthorised email address to access personal data; and

4.2.6 Leaving paper documents containing personal data in a place accessible to other people.

5 Internal Communication

Reporting a data breach upon discovery

5.1 If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Data Protection Officer ("the DPO") immediately:

Cathy Brown
Head of Governance and DPO
TMET
The Mead Centre, 343 Gipsy Lane, Leicester, LE4 9DD
0116 2143148 / 07970 980952
dpo@tmet.uk

5.2 The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

5.3 If it is considered to be necessary to report a data breach to the ICO then the Trust must do so within 72 hours of discovery of the breach.

5.4 The Trust may also be contractually required to notify other organisations of the breach within a period following discovery.

5.5 It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the DPO immediately.

5.6 Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

5.7 In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation

5.8 The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any **personal data**. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

5.8.1 remote deactivation of mobile devices;

5.8.2 shutting down IT systems;

5.8.3 contacting individuals to whom the information has been disclosed and asking them to delete the information; and

5.8.4 recovering lost data.

Breach investigation

5.9 When the academy/Trust has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

5.10 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

5.10.1 what data/systems were accessed;

5.10.2 how the access occurred;

5.10.3 how to fix vulnerabilities in the compromised processes or systems;

5.10.4 how to address failings in controls or processes.

5.11 Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis

5.12 In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform the DPO as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

5.13 Such an analysis must include:

5.13.1 the type and volume of **personal data** which was involved in the data breach;

5.13.2 whether any **special category personal data** was involved;

5.13.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

5.13.4 the security in place in relation to the **personal data**, including whether it was encrypted;

5.13.5 the risks of damage or distress to the **data subject**.

5.14 The breach notification form annexed to this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the Trust in deciding whether or not to report the breach.

6 External communication

6.1 All external communication is to be managed and overseen by the DPO and academy principal (where appropriate).

Law enforcement

6.2 The DPO and academy principal (where appropriate) will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

6.3 The DPO and academy principal (where appropriate) shall coordinate communications with any law enforcement agency.

Other organisations

6.4 If the data breach involves **personal data** which we process on behalf of other organisations, then we may be contractually required to notify them of the data breach.

6.5 The Trust will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

6.6 If the Trust is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then the Trust has 72 hours to notify the ICO if the data breach is determined to be notifiable.

6.7 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

6.7.1 the type and volume of **personal data** which was involved in the data breach;

6.7.2 whether any **special category personal data** was involved;

6.7.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

6.7.4 the security in place in relation to the **personal data**, including whether it was encrypted;

6.7.5 the risks of damage or distress to the **data subject**.

6.8 If a notification to the ICO is required, then see part 8 of this policy.

Other supervisory authorities

6.9 If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

6.10 When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by the Trust.

6.11 The communication will be coordinated by the DPO and will include at least the following information:

6.11.1 a description in clear and plain language of the nature of the data breach;

6.11.2 the name and contact details of the DPO;

6.11.3 the likely consequences of the data breach;

6.11.4 the measures taken or proposed to be taken by academy/Trust to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

6.12 There is no legal requirement to notify any individual if any of the following conditions are met:

6.12.1 appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);

6.12.2 measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

6.12.3 it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

6.13 For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Press

6.14 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

6.15 All press enquiries shall be directed to the Trust office as set out in the Trust Media and Press Policy.

7 Producing a Breach Notification Report

7.1 All members of our **workforce** are responsible for sharing all information relating to a data breach with the DPO, which will enable the annexed Breach Notification Report Form to be completed. This is an internal form which will be completed for all data breaches. If a report to the ICO is required, the DPO will use the information in this form to do so.

7.2 The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

7.3 If any member of our **workforce** is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

7.4 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

8 Reporting to the ICO

8.1 The DPO will report the breach to the ICO if it is considered that it is likely that the breach will result in risk to people's rights and freedoms.

8.2 The ICO provide a helpline to offer advice on a data breach and what to do next: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

8.3 If the advice from the helpline is to report to the ICO (or if the DPO is confident to report directly without consulting the helpline or if this is an initial report pending further investigation), the DPO should submit a completed ICO 'Report a personal data breach' form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

9 Evaluation and response

9.1 Reporting is not the final step in relation to a data breach. The academy/Trust will seek to learn from any data breach.

9.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

ANNEX 1 – TRUST DATA BREACH NOTIFICATION REPORT

Please complete as much of this form as possible and send to the DPO as soon as possible after reporting the breach to the DPO. If you wish to discuss any aspect of the form before submitting, please contact the DPO.

1 **About you** (the person completing this form)

Name	
Role	
Name of academy (or Trust, Teaching School or SCITT)	
When was the last data protection training/briefing you had	

2 About the breach

When did you discover the breach? (date and time)
When did the breach happen? (date and time)
Describe as much as you can about what happened, what went wrong and how it happened.
What sort of personal data was included in the breach? (highlight any that apply) Data revealing racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Sex life data Sexual orientation data Gender reassignment data Health data Basic personal identifiers, e.g. name, contact details Identification data, e.g. usernames, passwords Economic and financial data, e.g. credit card numbers, bank details Official documents, e.g. driving licences Location data Genetic or biometric data Criminal convictions, offences Not yet known Other (please give details below)
How many personal data records are concerned?
How many people's personal data are concerned?

What sort of people are affected? I.e. the people whose personal data are involved in the breach. *E.g. pupils, academy staff, parents*
What are the potential consequences and adverse effects of the breach? *E.g. reputation, emotional distress, fraud, identity theft, implications for their employment*
Has there been any harm to an individual? *E.g. a complaint about the incident.*

3 Taking action

What actions have you already taken as a result of the breach? To minimise/mitigate the effect on the affected individuals and/or to recover the data. *E.g. disabled email account, confirmed data sent in error has been destroyed, updated passwords.*
What actions have you identified to take to prevent a recurrence of this type of breach? *E.g. staff training, change naming of email distribution lists, change or tighten up procedures.*
Do the affected individuals know about the breach?
Have you told any other organisations about the breach? *E.g. the police, regulators or supervisory authorities.*

ANNEX 2 - DEFINITIONS

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an 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.
Data Controllers	are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes, any individual employed by the Trust such as staff and those who volunteer in any capacity including Governors, Trustees, Members and parent helpers.