Data Breach Policy

Originator:	Data Protection Officer
Responsible sub-committee:	Risk and Governance Committee
Linked Policies:	Data Protection Policy Subject Access Request Policy Data Retention Policy
Review Date:	June 2026
Target audience:	All stakeholders in the Trust
Dissemination via:	Email, SharePoint, Website

Version	Section	Amendments	Date	Author
1.0	**n/a**	**New document –**	May 2018	Data Protection Officer
1.1	**Section 9 (responsibilities) added**	Data Protection Officer details updated Breaches Log format updated	June 2021	Data Protection Officer
1.2	**Entire policy**	**Removal of forms for reporting** **Addition of flowchart for reporting**	July 2023	Data Protection Officer

Contents

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** 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 our **workforce** on how to deal with a suspected or identified data breach.

2.2 In the event of a suspected or identified breach, the 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 Commissioners 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 Trust and for **data subjects** including:

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

2.5.2 Reputational damage to the 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;

4.2.4 Sending an email or attachment to the wrong recipient;

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 at

dataprotectionofficer@inovamat.org

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 make the 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 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.

5.8 A summary of all breaches log (*Annex 2*) will be maintained and reported to C-Suite monthly and Trustees on an at least an annual basis.

Breach minimisation:

5.10 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:

5.10.1 Remote deactivation of mobile devices;

5.10.2 Shutting down IT systems;

5.10.3 Taking systems offline;

5.10.4 Retrieving any lost, stolen or otherwise unaccounted for data;

5.10.5 Restricting access to systems entirely or to a small group;

5.10.6 Backing up all existing data and storing it in a safe location;

5.10.7 Reviewing basic security, including:

- Changing passwords and login details on electronic equipment
- Ensuring access to places where data is kept is monitored and requires authorisation - Restrict file access;

5.10.8 Contacting individuals to whom the information has been disclosed and asking them to delete the information; and

5.10.9 Recovering lost data.

Breach investigation:

5.11 When the 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.

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

5.12.1 What data/systems were accessed;

5.12.2 How the access occurred;

5.12.3 How to fix vulnerabilities in the compromised processes or systems;

5.12.4 How to address failings in controls or processes.

5.13 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:

5.14 To determine the seriousness of a data breach and its potential impact on **data subjects**, and to inform the Trust 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.

5.15 Such an analysis must include:

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

5.15.2 Whether any **special category personal data** was involved;

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

5.15.4 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**. This could include risks to the following:

- Physical safety
- Emotional wellbeing
- Reputation
- Finances
- Identity
- Private affairs becoming public

6   External communication

6.1 All external communication is to be managed and overseen by the DPO.

Law Enforcement

6.2 The DPO 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 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 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 assess the data breach against the following criteria considering 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 9 of this policy below.

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 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 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 Trust Marketing & Communications Lead:

media@inovamat.org

7   Notifying the DPO of the data breach

7.1 All members of our **workforce** are responsible for sharing all information relating to a data breach with the DPO.

7.2 The DPO may ask the individual further questions when notified of a data breach.

8   Evaluation and response

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

8.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again.

8.3 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.

9 Responsibilities

9.1 Staff Members:

9.1.1 Each and every staff member is responsible for identifying personal data breaches and reporting breaches to the Data Protection Officer (DPO) by emailing dataprotectionofficer@inovamat.org

9.1.2 Staff members are responsible for providing any requested information about the breach to the DPO so the DPO can fulfil their responsibilities.

9.1.3 Staff members are responsible for assisting the DPO with subsequent breach investigations.

9.2 Data Protection Officer:

9.2.1 The DPO is responsible for logging all Personal Data Breaches on the Trust Breach Register.

9.2.2 The DPO is responsible for coordinating investigations into the Personal Data Breaches

9.2.3 The DPO is responsible for risk assessing the breach to determine whether the breach meets the threshold to report to the Information Commissioner's Office

9.2.4 Where a breach is determined to be reportable to the ICO, the ICO requires that the Trust send the completed Breach Report to casework@ico.org.uk with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. This is the DPO's responsibility.

9.2.5 The DPO Is responsible for identifying improvements and any remedial actions following a breach

9.2.6 The DPO is responsible for closing a personal data breach.

10 Annex 1 - 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, 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 way, 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 Trust such as staff and those who volunteer in any capacity including Governors, Trustees, Members, Volunteers, and parent helpers.

11 Annex 2 - Trust Breaches log

This document is a summary of all breaches and their status. The report will be reviewed by C-Suite monthly and by Trustees at least annually.

[TSAT Breach Register.xlsx (sharepoint.com)](TSAT Breach Register.xlsx)

12 Annex 3 - Data Breach Flowchart

A staff member recognises that a potential personal data breach has occured

The staff member immediately notifies the Data Protection Officer (DPO) at dataprotectionofficer@taptontrust.org.uk

Please note, that as all personal data breaches are unique in their nature, we may need to deal with some incidents with a slightly different process than listed here. This is a guide only.

The DPO may ask further questions to the staff member to better determine what has happened

Where the DPO determines that the reported incident is not a personal data breach, the DPO will communicate this to the staff member along with any necessary steps to take

If this incident is classified as a 'near miss', this will be logged on the TSAT Breach Register

From an initial review of the information provided, the DPO will determine whether further individuals should be involved, such as the Business/Office/School Manager, headteacher, IT Director, Deputy CEO or any other relevant individual

The DPO will initiate the 'Breach Minimisation' steps outlined in Part 5 of the Data Breach Policy. This includes steps to minimise the effects of the incident

The DPO along with relevant members of staff, will conduct an investigation into the incident as detailed in Part 5 of the Data Breach Policy

Where the Trust is a Data Processor for the data (although this is not usually the case), the DPO will ensure that the Data Controller is notified of the incident and will co-operate with any further necessary steps

The DPO along with relevant staff members will determine whether the incident will be reported to the ICO and the data subjects affected

Risk

High risk

Unlikely to result in risk

Where it is determined that there is a risk to the rights and freedoms of the individuals, the DPO will prepare and send a report to the ICO within 72 hours

Where it is determined that there is a high risk to the rights and freedoms of the individuals, as well as informing the ICO, the DPO will prepare and send a communication to the data subjects affected without undue delay

Where it is determined that it is unlikely to result in a risk to the rights and freedoms of the individuals, the incident will not be reported to the ICO or affected data subjects, unless the Trust wishes to do so (this is not legally required)

The DPO is responsible for notifying any other outside organisations of the incident where required

Following any data breach, the Trust will ensure that steps are put in place to prevent the incident occuring again

The DPO will ensure that all information relating to the data breach is logged on the TSAT Breach Register, as referenced in Annex 2 of the Data Breach Policy and then close the incident

10