Reporting a Data Breach Procedure

Responsible Manager:	Director of MIS	**Date:**	June 2024
Approved by:	Information Governance Group	**Approval Date:**	Expected June 2024
GDPR Lead:	DPO	**Review Date:**	June 2026

Accessible to Clients/ Students:	Yes

1. Applicability to Organisation

The Data Breach process applies to:

The Trafford and Stockport College Group

2. Scope and Purpose

This process covers all data processed by and for The Trafford and Stockport College Group

3. Approach

The Data Breach process sets out the process and timescales for reporting breaches or addressing near misses of personal information.

4. Linked Policies

Data Protection Policy

5. Linked Procedures

Information Security Procedures

6. Equal Opportunities Statement

No impact on equality has been identified.

7. Location and Access

The Data Breach process is located as follows:

Group website Guide to Information: Our policies & procedures

Group intranet Group Policies and Procedures

8. Person Responsible for the Data Breach process document

Data Protection Officer (DPO)

9. Variations

There are no variations to the Data Breach process.

Where do I report a data breach or "near misses"?

If you think there has been a data breach, immediately report this to the **DPO, Sofia Carroll of Naomi Korn Associates (Outsourced data protection support)**Via the breach reporting form on SharePoint https://livetraffordac.sharepoint.com/sites/GDPRInformationSecurity?e=1%3A5a28756c09f44f67aa77ecadccf748bc . The form will automatically and immediately inform the DPO the form has been submitted by a member of staff.

You can also email the DPO directly at dpo@tscg.ac.uk with any concerns or questions.

A data breach could be as simple as you putting a letter in the wrong envelope and therefore even the most minor data breaches must be reported.

False alarms or even breaches that do not cause any harm to individuals or to the Group should nevertheless be reported as it will enable us to learn lessons in how we respond and the remedial action we put in place.

Many people would recognise that a near miss is a situation where the accidental recipient would already have had access to the information shared, the information shared is trivial, or a misdirected email contains only a link that the recipient would not be able to access. It also covers situations where unauthorised access was possible but was not exploited. All are, however, breaches and need to be reported and lessons learnt on how to avoid them in the future.

We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you **do report** any breach, even if you are unsure whether or not it is a breach. Reporting of near misses helps to identify and rectify flaws in systems and processes that could lead to a more substantive breach with serious consequences.

What is a Data Breach?

A data breach is a security incident in which personal or other confidential information data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so.

- Data means information in any format, e.g., papers, records, emails, faxes, texts etc.The definition of personal data is wide and can be complex and includes any information that identifies a living person and concerns or affects them in some way.

Examples of breaches and “near misses”

While this list is non-exhaustive it does give examples of some of the more common data breaches and 'near misses' that should be reported.

- leaving paper records on a train;
- email personal data to the wrong person;
- deleting personal data when it is still needed;
- losing a memory stick containing personal data;
- loss or theft of mobile devices containing data about people (e.g., laptops, PDAs, mobile phones, etc.) or loss of hard copy data within briefcases, folders;
- sharing information about people with unauthorised third parties, either accidentally or willfully;
- providing means of access to an unauthorised individual through provision of a password or granting of permissions;
- Data is made unavailable or inaccessiblle;
- sending emails or letters in error to the wrong person(s) or wrong address (es); and
- any 'near miss' incident that had the potential to cause a data breach even though it might not have done so.

Mitigation and management of personal data breaches

The DPO, supported by other team member if needed, will review the breach, decide on how to manage it, assess whether it is necessary to invoke any emergency reposnses and take any decision on external reporting.

It may also be necessary to consider notifying third parties such as the police, insurers, professional bodies, regulatory authorities, or bank or credit card companies which can help reduce the risk of financial loss to individuals.

Where a system is involved that is provided externally, then the supplier may be required to undertake an investigation into the causes of the breach and set out a plan for remediation. Reporting of breaches discovered by suppliers is a requirement of the Group’s contract with them.

Note that malicious breaches, where the breach is caused by an individual knowingly and purposely flouting the Data Protection legislation and the Group’s relevant policy, this should be escalated to the DPO and/or HR as appropriate.

The decision to inform data subjects of the breach must be taken without undue delay. Such communications such include:

- the name and contact details of the DPO
- a description of what data has been lost and the consequences
- a description of the measures to address the breach taken by [INSERT]
- if relevant, any advice to individuals on steps they can take, such as a password reset or cancelling a credit card

Steps required to contain and mitigate the breach will be identified, documented and undertaken.

These may include:

- immediately recalling an email that has been sent to the wrong address;
- contacting the recipient of an email that has been sent in error and asking them to delete the email from their inbox and deleted items and confirm they have done so;
- immediately retrieving paper documents from any unintended recipients;
- changing the password for the affected application, device, system or room;
- immediately disabling any lost or stolen electronic devices;

- notifying colleagues of any immediate steps that they should take;
- remotely locating, disabling and/or deleting data stored on a mobile device;
- restoring a database or system from a back-up;
- disabling network or system access; and
- notifying staff and/or Processors to do or refrain from doing something.

All actions need to be appropriate, proportionate and accountable.

Why should breaches be reported?

The longer an incident goes unreported, the longer a vulnerability may remain unaddressed allowing the incident to escalate or for further incidents to occur.

There is a hard regulatory deadline for reporting serious breaches posing high risk to personal data to the the ICO within 72 hours of becoming aware of them.

Without timely visibility of the incident through reporting we may not be able to fulfil legal obligations.

The UK GDPR places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office. Knowing that a breach has occurred and delaying reporting reduces the time available for the investigation team to understand and assist with a response and still meet legal compliance. Where the breach does not affect personal data, time is still critical and may have contractual implications.

Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust and so prevent future breaches.

Who should report?

All employees, contractors and temporary workers.

What happens after the report is made?

Immediately after the breach has been identified and the approach to managing the breach agreed there will be immediate actions that should be taken, such as:

- contacting an unauthorised recipient
- retrieving or deleting a mis-sent email
- taking down a hacked website

In the post breach period remedial action such as review of processes should be undertaken and a lessons learned approach implemented so the Group can avoid similar incidents occurring in future. Remedial measures may include:

- training
- security review
- new procedures
- amending risk registers

It is a requirement to document the facts relating to the breach, its effects and the remedial action taken. This is part of the overall obligation to comply with the accountability principle and allows the ICO to verify compliance with its notification duties under the data protection legislation.

When an incident is reported the DPO will provide advice and guidance. This will include advice on communications to the individuals(s) whose personal information has been affected. It will also include advice on if the breach is reportable to the ICO and identifying the cause or the breach.

Factors to consider in assessing risk include:

- The type of breach
- The nature, sensitivity, and volume of personal data
- Ease of identification of individuals
- Severity of consequences for individuals
- Special characteristics of the individual e.g. children and vulnerable adults
- Special characteristics of the Data Controller e.g. if holding sensitive medical data
- The number of affected individuals

The DPO, with the assistance of colleagues if needed, will also consider if the breach results in any of the following for the affected data subjects:

- Loss of control over personal data
- Limitation of rights
- Discrimination
- Identity theft or fraud
- Financial Loss
- Damage to reputation
- Breach of confidentiality
- A safeguarding or wellbeing risk
- Reverse of pseudonymisation

Where the breach will result in a high risk to the individuals affected, the Group is required to notify the Information Commissioner’s Office within 72 hours of becoming aware of the breach. Not all data breaches will reach the threshold for notification.

Where an incident is to be reported to the ICO the Data Protection Officer, the Chief Finance Officer and Director of IT will be aware that this decision has been taken and one of the named roles will complete the report. In most instances it will be the DPO who reports the breach to the ICO. If it appears that there is a high risk to individuals, even if all the information is not yet available, a report should be made to the ICO in relation to what [is known at that time.

Reports can be made on the ICO website via email by completing their downloadable form. The DPO will submit a report if required.

If the decision not to report to the ICO is made the reasons for this should be recorded and the breach logged in the standard manner.