Data Breach Procedure

Table of Contents

Data Breach Procedure

1.0 Purpose

Talented Training Ltd collects, holds, processes, and shares information and we are aware personal information is an asset. We must protect all personally identifiable information we hold from either accidental or deliberate incidents, which could lead to a data protection breach.

We are obliged under Data Protection legislation to have in place a framework designed to ensure the security of all personal information, including clear lines of responsibility.

This procedure must be followed to ensure a consistent and effective approach is in place for managing data breaches across Talented Training Ltd. It relates to all personal and sensitive personal information held by us regardless of format. The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal information and prevent further breaches.

Please note that the following inter-changeable terms are used throughout this document:

- Personal data and personally identifiable information
- Data subject and individual
- Regulator and Information Commissioners Office – ICO

1.1 Scope

This policy shall apply to all employees, learners, and other stakeholders of Talented Training Ltd, including temporary, casual or agency staff and consultants, suppliers, and data processors working for, or on behalf of Talented Training Ltd.

2.0 Reporting Procedure

We recognise damage limitation is a priority immediately following a security incident/breach.

Any individual who accesses, uses, or manages Talented Training Ltd information/data is responsible for reporting a data breach and security incidents immediately to the Management Team.

If a breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable possible to the Management Team.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting, the nature of the information, and how many individuals are involved. A Data Breach Report should be completed by filling in this Data Protection Submission Form.

The report will enable the Data Protection Team to make the decision as to whether to

inform any affected individuals and the Information Commissioners' Office (ICO), about the breach. The time limit for notifying the ICO is 72 hours from becoming aware of the breach and it is best practice to inform the regulator first before communicating with those affected. Therefore, any individual reporting a breach or security incident must act with urgency and provide as much information as possible in the Data Protection Submission Form.

3.0 Preliminary Assessment, Containment and Recovery

The Management Team will take steps, within the first 24 hours of the incident (where possible) to carry out a preliminary assessment of what data has been lost, why and how. Containment and recovery will then become the priority.

The Management Team will attempt to contain the breach or determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise further loss, destruction, or unauthorised disclosure of data. The Management Team may need to notify Talented Training's insurers and, if the breach arises out of a criminal event, notify the police and the National Cyber Security Centre.

4.0 Investigation and Risk Assessment

Having dealt with the immediate aftermath of the data breach, the Management Team will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for the data subjects, how serious or substantial those are and how likely they are to occur.

The investigation will need to consider the following:

- The type of data involved.
- Its sensitivity.
- The risk of harm of the data subject.
- What security measures or procedures are in place (e.g., passwords/encryptions).
- What has happened to the data (e.g., has it been lost or stolen).
- Whether the data could be put to any illegal or inappropriate use.
- The individuals affected by the breach, number of individuals involved and the potential effects on those individual(s).
- Whether there are any wider consequences to the breach.

5.0 Notification

Every incident will be assessed on a case-by-case basis. The dangers of over notifying must be considered. Not every incident warrants a notification and over notification may cause disproportionate queries and work.

The Management Team will establish whether the ICO will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible. Where there is no risk to the rights and freedoms of the data subjects, the regulator will not be notified.

The Management Team will also establish whether any affected data subjects need to be

notified. As above, this notification is only required where the breach is likely to result in a high risk to the rights and freedoms of those data subjects. Talented Training Ltd is required to notify the ICO without undue delay, but after notification to the regulator, it is best practice to notify those affected and include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks by Talented Training Ltd.

The Management Team will consider whether anyone else will require notification, e.g., a business party pursuant to a contractual obligation. They also must consider notifying third parties such as the police, insurers, banks, or credit card companies. This is appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

6.0 Evaluation and Response

Once the initial incident is contained, the Management Team will conduct a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where personal data is held and how it is processed.
- Where the biggest risks lie, including potential weak points within existing security measures.
- Whether methods of transmission are secure, sharing minimum amount of data necessary.
- Whether additional employee awareness training is required.

If deemed necessary, the Management Team will implement any changes to systems, policies, and procedures, following the outcome of the review.

7.0 Consequences of Failing to Comply

The company takes compliance with this procedure very seriously. Failure to comply with the procedure:

- Puts at risk the individuals whose personal information has been exposed.
- Carries the risk of significant civil and criminal sanctions for the individual and the Company
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this procedure, failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct.

If a non-employee breaches this procedure, they may have their contract terminated with immediate effect.

8.0 Definitions

Personal data - means information relating to an individual who can be identified (directly or indirectly) from that information. Data that, if lost or stolen, would be likely to cause damage or distress to one or more individuals. This includes, but is not limited to, bank details, human resources data and exam or assessment results which are not a matter of public record.

Criminal offence data – means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Data subject – means the individual to whom the personally data relates.

Processing information – means obtaining, recording, organising, storing, amending, retrieving, disclosing and / or destroying information, or using or doing anything with it.

Special category information – (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Information Commissioners Office - Is the UK's independent regulator for data protection and upholding information rights and data privacy for individuals. ICO can act against organisations and individuals that collect, use, and keep personal information. This includes criminal prosecution, non-criminal enforcement, and audit.

9.0 Document Control

Below is the change history and document 'sign off' information.

9.1 Version Control

Record of Amendments		
Version Number	**Date of Issue**	**Detail of Change**
V1.0	**May 2025**	**Document created.**

9.2 Next Review Date

The next scheduled review of this document will be May 2026 or earlier if there is a need for an additional review.

9.3 Document Authorisation

Document Authorisation		
Name and Position	**Signature**	**Date**
Laura Jambawai **Quality and Adult Skills Lead**	**LJambawai**	**27 May 2025**