Ginger Nut Training.

Document Title

Process for Reporting Data Breaches

Originator	Responsible Person
Directors	Directors

Date of Approval	Policy Due for Renewal
August 2024	July 2025

Version 10.1.0

Ginger Nut Training
37 Queen Street, Colchester, CO1 2PQ
www.gingernuttraining.co.uk

Process for Reporting Data Breaches

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

What you need to do

If you become aware of, or suspect, any data breach taking place then you must immediately (or as soon as possible) inform your line manager or the director responsible of this breach. You will be expected to give full and accurate explanation of what has happened and how it happened.

Responsible Directors

Data Protection Officer - Dan Williams – 07834 554 379
Director with responsibility for IT – Harry Simpson – 07860 590 568

What we will do

Once a data breach has been identified we will work with TCS to understand the risks of what has occurred, any data that has been breached and the level of risk in that data. We will also carry out any steps that are required to mitigate this.

Where the consequences of the breach are assessed to be 'High Risk' we will, as quickly as possible inform the individuals affected, their employer (where appropriate) and the ICO.

What information must we provide to individuals when telling them about a breach?

We will describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of our data protection officer, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, we will give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:

- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

What information must we provide to employers when telling them about a breach?

We will describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of our data protection officer, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.
- Details of which employees were included in the breach

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see pages on reporting a breach. These pages include a self-assessment tool and some personal data breach examples.

How much time do we have to report a breach?

We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have 'become aware' of a breach.

What information must a breach notification to the ICO contain?

Breaches should be reported to the ICO via their online form at - https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/report-a-data-breach-online-form/

The form must be submitted in one go and cannot be saved, so all relevant details must be prepared before submission.

Information to report will cover:

- what has happened;
- when and how we found out about the breach;
- the people that have been or may be affected by the breach;
- what we are doing as a result of the breach; and
- who the ICO should contact if we need more information and who else you have told.

We will ensure the information provided is accurate and supply the ICO with as much detail as possible.

What if we don't have all the required information available yet?

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

We must still notify ICO of the breach when we become aware of it and submit further information as soon as possible. If we know we won't be able to provide full details within 72

hours, we will explain the delay to them and tell them when we expect to submit more information.

Example

We detect an intrusion into our network and become aware that files containing personal data have been accessed, but you don't know how the attacker gained entry, to what extent that data was accessed, or whether the attacker also copied the data from your system.

We notify the ICO within 72 hours of becoming aware of the breach, explaining that we don't yet have all the relevant details, but that we expect to have the results of our investigation within a few days. Once our investigation uncovers details about the incident, we give the ICO more information about the breach without delay.

What else do we need to do after a breach

We must ensure that we record all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires us to document the facts regarding the breach, its effects and the remedial action taken. This is part of our overall obligation to comply with the accountability

principle, and allows the ICO to verify our compliance with its notification duties under the UK GDPR.

As with any security incident, we will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented. Human error is the leading cause of reported data breaches. To reduce the risk of this, we will consider:

- mandatory data protection induction and refresher training;
- support and supervising until employees are proficient in their role.
- updating policies and procedures for employees should feel able to report incidents of near misses;
- working to a principle of "check twice, send once";
- implementing a culture of trust – employees should feel able to report incidents of near misses;
- investigating the root causes of breaches and near misses; and
- protecting your employees and the personal data we are responsible for. This could include:
  - Restricting access and auditing systems, or
  - Implementing technical and organisational measures, eg disabling autofill.

Further Resources

- Responding to a cybersecurity incident (ICO) - https://ico.org.uk/media/for-organisations/documents/2614816/responding-to-a-cybersecurity-incident.pdf
- Self Assessment on whether breach requires reporting - https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment/
- Data Breach Reporting (ICO) - https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/