DATA BREACHES – INFORMATION AND REPORTING PROCEDURE

Overview

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. It can take many forms. Examples of data breaches include:

- loss or theft of data
- unauthorised access to, use of, or modification of data
- equipment damage
- human error
- malicious intent
- loss or theft of equipment.
- System hacking (including emails)
- Careless disposal of used computer equipment or data storage media

This list is not exclusive.

Where data is disclosed legally and staff are authorised to do so, this procedure does not apply, however all disclosures, including those which are legal and authorised must be recorded in the appropriate log. All staff must be made aware of the existence of this log.

A breach can impact business transactions and staff's ability to work, it can also harm our reputation, but the risk in a personal data breach is to the data subjects.

The GPDR brings in a requirement to report a personal data breach to the Information Commissioner’s Office (ICO) unless you can demonstrate it's unlikely to result in a risk to individuals rights and freedoms.

In most cases the ICO reporting team will give recommendations to help put better measures in place to help prevent similar breaches in the future.

If a breach is serious, complex or involves a cyber incident they may need to carry out an in-depth investigation.

Preventing unauthorised disclosure and minimising risk:

- All staff will be trained in data protection.
- All staff will read related policies and procedures.
- An investigation will be carried out for every breach or near miss reported.

Responsibility of all employees and Board members:

- As soon as any employee or Board member suspects or discovers that an actual breach has occurred this must be reported to the Chief Executive Officer or the Operations Manager (Data Protection Information Officer).
- Near misses must also be reported.
- You must give as much detail as you can.

Responsibility of the persons responsible for data protection (Chief Executive Officer, with the assistance of the Data Protection Information Officer (DPIO)).

It is the responsibility of the CEO to contain the breach and help the organisation recover from the impact. In the absence of the CEO, the Operations Manager (DPIO) will assume responsibility.

Procedure and guidance for CEO:

1. The CEO should start and complete a Data Breach Record form in the event of a known or suspected breach of personal/sensitive information. During the investigation and after completion, this should be filed on the GDPR file.

Reporting
Record.docx

2. **Assess the risk**, both to data subject/s and the organisation; remember the primary risk in a personal data breach is to the data subject. Think about how this breach could cause these people harm. How sensitive is the data? Could this breach lead to distress, financial or even physical harm? Decide whether there any safeguards in place that could lower the risk? For example, is the data encrypted? Has it gone to a trusted body?

3. **If there are more safeguards you can put in place now, do so now.**

4. **Decide who should be informed** – including the ICO, the data subjects, industry regulators and the police, or IT personnel or providers. If there is a high risk to individuals' rights and freedoms you will need to notify them. In fact, the ICO may require you to.

5. **If by informing data subjects or IT providers (for example) IMMEDIATELY, the incident may be contained or harm reduced, inform them now.**

6. **Provide instruction to staff on steps to contain the breach**, for example changing passwords, shutting computers down or halting network traffic.

7. **Put immediate safeguards in place** and, for example, provide instruction and authorisation to restore data from backups if that's the issue and is possible.

8. **Report the breach if necessary.** If a breach needs to be reported this must be done within 72 hours of the breach being discovered. During office hours call the ICO specialist team on 0303 123 1113. They will work with you to understand what's happened, get all of the information they need and help with the next steps.

If you need to report and you can't reach the ICO on the phone, if you already have a written report ready, or you have relevant documentation to send you can report via the ICO website:

https://ico.org.uk/for-organisations/report-a-breach/

- **Remember to record all investigations and decisions**
- **Ensure that the breach or near miss is added to the Board agenda**

What information will the ICO need?

- How many people could be affected and how many records?
- What type of data has been breached?
- Is there any sensitive information?
- What did you have in place that could have stopped it?
- Are your staff trained?
- What steps have you taken so far to safeguard the data subjects?

- Are there any more steps you will take?
- Are policies and procedures in place. Are they written down?
- Security measures you have in place.
- Are staff are trained in the processes the organisation uses and if you provide guidance for them that they can use as a reference?
- What have you learned from this breach?
- How can you improve your practices?
- What have you done or will you do to stop a similar incident from happening again?