Data Breach Reporting Procedure

Guidance

- General Data Protection regulations (2018)
- ICO

What is a data breach?

The ICO sets out that a personal data breach is, '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.

Examples of data breaches include:

- ***access by an unauthorised third party;***

e.g., An address on a letter is incorrect and gets sent to the wrong person meaning that personal data within that letter is being accessed by an unauthorised third party.

- ***deliberate or accidental action (or inaction) by a controller or processor;***

e.g.

- ***sending personal data to an incorrect recipient;***

e.g., Emailing 'reply all' resulting in personal data being shared with incorrect recipients.

- ***computing devices containing personal data being lost or stolen i.e. USB, iPad, Laptops etc;***

e.g., You have taken home an organisational laptop and on the way home stopped at the shops, where your car is broken into and the laptop stolen.

- ***alteration of personal data without permission;***

e.g., A friend has told you a person's mobile number and you add them to tapestry without their explicit consent.

- ***loss of availability of personal data.***

e.g., Someone has given you their details to add to tapestry or Donorfy, but you have lost the piece of paper you have written them on.

Organisational Responsibilities

The ICO confirms that under the GDPR, they should be notified of certain types of data protection breaches and that these should be reported without undue delay and within 72 hours of becoming aware of the breach, where feasible (even if you don't have all of the details yet).

Dingley's Promise will report to the ICO any breach that.

- poses a high risk of adversely affecting individuals' rights and freedoms.

Where a data breach is required to be reported to the ICO, the following information must be included:

- A description of the nature of the breach.
- The categories of personal data affected.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.
- Name and contact details of the Data Protection Officer.
- Consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.

Responsibilities

When a breach has occurred, and as soon as you are made aware of it you should.
- report the breach to your line manager in the first instance as soon as the breach occurs and email the DPO on **dpo@dingley.org.uk** and phone the Chief Operating Officer, or in his absence, the Chief Executive Officer within 1 hour of the breach.

The DPO will;
- establish the likelihood and severity of the resulting risk to people's rights and freedoms based on how serious and substantial these are, and how likely they are to happen.
- where applicable, notify the ICO if it is a serious breach, and notify the data subject/s

The Chief Operating Officer will document full details of all reported breaches, including those not reported to the ICO, with justification as to why. This will be kept in a secure folder on our internal cloud system.

Following any data breaches, whether or not they are reported to the ICO, subsequent measures will be taken to ensure that a similar breach is less likely to occur.

Contact Details

Lee Friend, Chief Operating Officer

Tel: 07388943455

Email: Lee.Friend@dingley.org.uk

Catherine McLeod, Chief Executive Officer

Tel 07946226030

Email: Catherine.Mcleod@dingley.org