Title of policy: Data Breach

Unique ref number: CEOP03

Directorate: Office of the CEO

Department: Data Protection

Table of Contents:

Please note: this document contains links to other documents

1. Purpose:

Organisations are required to have robust procedures in place to ensure that they can identify data incidents, investigate the causes, decide whether it is a data breach under the GDPR (General Data Protection Regulation) and respond quickly to implement measures to minimise the impact on the data subjects and to prevent recurrence.

This breach procedure sets out the course of action to be followed by all staff within GuideDogs (hereafter, GDBA) if a data incident takes place.

Under the DPA (Data Protection Act 1998), notification to the ICO (Information Commissioner's Office) was voluntary rather than mandatory. This is not the case under the GDPR and all data breaches which have the potential to have a significant detrimental effect on the individual(s) through discrimination, damage to reputation, financial loss, loss of confidentiality, or any other economic or social disadvantage must be reported by the data controller to the ICO within 72 hours of discovery.

If the breach is 'high risk' to the individual(s) affected then GDBA must also notify the data subject(s).

In order to effectively monitor data incidents, the DPO (Data Protection Officer) will document each data incident in the Data Breach Log file, including facts of the incidents, the effects and action taken and will note if the incident had been escalated to a data breach that is reportable to the ICO.

Remember: If you discover a data incident, immediately inform the Data Protection Officer, Phillippa Caine, at dataprotectionofficer@guidedogs.org.uk **or** Phillippa.caine@guidedogs.org.uk

2. To whom the policy applies:

All employees, volunteers, workers and contractors are required to comply with the provisions of this Policy.

3. Main principles:

Types of Breach

Data incidents occur for a wide variety of reasons, including loss or theft of equipment, unauthorised access to data, unforeseen circumstances such as fires or flooding and the majority (over 80%) are caused by errors/carelessness rather than hacking or viruses.

Some examples are:

- Loss or theft of staff or customer data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- Blagging' offences where information is obtained by deception.

GDBA Process in the event of a Data Incident

In discovery of a data incident, the following steps should be followed:

1. The person who discovers/receives a report of a data incident must immediately inform the Data Protection Officer (dataprotectionofficer@guidedogs.org.uk). If the data incident occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The DPO will make an initial assessment of the severity of the incident to determine whether the data incident process needs to include the Executive Directors. The criteria for escalation includes:
    - Number of individuals affected
    - Nature of data incident (e.g. special categories of data / high risk data)
    - Significant technical incident – (e.g. lost unencrypted devices, hacked IT systems)

3. The DPO must ascertain whether the incident is still occurring. If so, steps must be taken immediately to minimise the effect of the incident. An example might be to shut down a system, or to alert any relevant external supplier.
4. The DPO will keep the CEO informed and depending on the severity of the incident, the Chairman and Trustees.
5. The DPO must also consider whether the Police need to be informed. This would be 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. The DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    - Attempting to recover lost equipment.
    - Contacting relevant authorities, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry

back. Whatever the outcome of the call, it should be reported immediately to the CIO (or nominated representative).
- The use of back-ups to restore lost/damaged/stolen data.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data incident includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

The DPO will coordinate response to the data incident and communications with the CEO, Chairman and other relevant members of GDBA as necessary throughout the course of handling the data incident.

Investigation

In most cases, the next stage would be for the DPO (or nominated representative) to fully investigate the incident. The DPO (or nominated representative) should ascertain whose data was involved in the incident, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

The investigation should consider:

- The type of data and whether it contains any special category data;
- Its sensitivity;
- What protections are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (customers, staff members, suppliers etc) and whether there are wider consequences to the breach.

If the investigation concludes that it is a significant breach then the Information Commissioner's Office (ICO) should be notified within 72 hours. Every incident should be considered on a case by case basis.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. Additional information can be reported through to the ICO as it is discovered during the course of the investigation, where the ICO has been notified about the data breach.

A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place, except in the event of a significant breach. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach.

The following points should be considered:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?

If a large number of people are affected, or there are potentially serious consequences, GDBA must notify the ICO with 72 hours. The ICO should only be notified if personal data is involved.

A breach notification to the ICO must include:

- The nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- Categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measure taken to mitigate any possible adverse effects.

There is guidance available from the ICO on when and how to notify them, which can be obtained at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-breaches/.

Review and Evaluation

Once the handling of the breach has been concluded, the DPO should fully review both the causes of the breach and the effectiveness of the response to it in order to:

1. Understand what can be done to prevent future breaches.
2. Determine how soon the changes can be implemented
3. Update and cascade training for employees as soon as possible.

4. The investigation should be written up and if the breach has been notified to the ICO, it will be shared with the Trustees. If systemic or ongoing problems are identified, then:
    - an action plan must be drawn up to correct the issues.
    - Where individuals have been notified of the breach, provide them with an update on the outcome of the investigation and what GDBA are doing to prevent future breaches.
    - If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.
    - A record of the breach will be kept by the Data Protection Officer.

5. Responsibilities:

The Data Protection Officer of Guide Dogs oversees the administration of this policy.
All staff, contractors and volunteers that have contact with Guide Dogs data have a responsibility to implement the Policy. Advice and guidance is available from the Data Protection Officer.

Guide Dogs will provide training, supervision and line management

6. Monitoring:

Legislation and Guidance that underpins the Data Breach Policy, Procedures and Processes.

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018

7. Related documentation:

Data Protection Policy

8. Document information:

- Owner: Phillippa Caine
- Job Title: Data Protection Officer
- Author: Phillippa Caine
- Job Title: Data Protection Officer
- Approved Date: April 2018
- Last Reviewed Date: April 2018
- Review Frequency: Every 2 years
- Next Review Due: April 2020

9. Version control table:

Please note the table below contains 2 rows and 5 columns. Other rows may be added as required.

Version No.	Detail of change / sign off	Author / Name	Position	Date
1.0		Phillippa Caine	Data Protection Officer	April 2018

End of document