Lighthouse Data Breach Policy Summary

Definition: A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes breaches that are the result of both accidental and deliberate causes.

Data protection breaches could be caused by several factors. Examples include: Loss or theft of child, staff, individual, or governing body data and/ or equipment on which data is stored; Inappropriate access controls allowing unauthorised use; Equipment Failure; Poor data destruction procedures; Human Error (e.g. sending personal information to an incorrect recipient); Cyber-attack; Hacking.

Managing a Data Breach

In the event that a breach is identified or is notified the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform The Data Lead or, in their absence, the Management. This should begin as soon as is practicable and certainly within 12 hours.
2. The Data Lead must only investigate sufficiently at this stage to decide how urgently a person or persons whose information has been accessed needs to be informed. E.g. if it is a loss of financial information this should be addressed urgently.
3. If the breach is still occurring, take steps to minimise the effect of the breach.
4. The Data Lead or nominated person must inform the Chair of Directors urgently.
5. The Data Lead or nominated person must also consider whether the Police need to be informed. (For instance, where illegal activity is known or likely)
6. The Data Lead or nominated person must quickly take appropriate steps to recover any losses and limit the damage. This might include:
    a. Attempting to recover lost equipment.
    b. Contacting any necessary organisations so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned.
    c. Consideration should be given to a global communication 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 by the Data Lead.
    d. The use of back-ups to restore lost/damaged/stolen data.
    e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and relevant agencies / staff informed.

Investigation

In most cases, the next stage would be for the Data Lead to fully investigate the breach. Ascertain whose data was involved in the breach, 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; Its sensitivity; What protections were 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 (children, staff, congregants, suppliers etc) and whether there are wider consequences to the breach.

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. A more detailed review of the causes of the breach and recommendations for future improvements can be done later.

Notification

Some people/agencies may need to be notified as part of the initial containment, usually once an initial investigation has taken place. The Data Lead should, after seeking expert or legal advice as needed, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. (24 hours if electronic.) Consider on a case by case basis.

When notifying affected individuals:

- Give specific, clear advice how they can protect themselves and how we can help.
- Give them opportunity to formally complain if they wish (see Complaints Procedure).
- Notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

If the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons notification may not be required.

In ALL cases information is to be documented.

Where the supervisory authority is not notified within 72 (24 if electronic) hours, it shall be accompanied by reasons for the delay.

The notification to ICO shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken (or proposed) to address the personal data breach, including, as appropriate, measures to mitigate its effects.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

In ALL cases document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Review and Evaluation

Once the initial aftermath is over the Data Lead should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and full Directors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to correct these.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Essential contacts

Organisation Data Lead: Dr. Harvey Grahame-Smith or management in his absence. Phone: 0780 3618375

Information Commission Office

Reference Number for ICO: Z7516662 www.ico.org.uk
Telephone: 0303 123 1113 to report a Breach or to ask for advice