

Lighthouse
Data Breach Policy
Part 2 of the Data Protection Policy

Purpose

This policy is intended to particularly cover areas around Data Breach.

The Data Protection Policy has three separate parts:

- 1. Main part**
- 2. Data Breach – this document**
- 3. Employee Data Protection**

Despite the procedures and process to be followed in the Data Protection Policy a Data Breach may occur

Policy Statement

The Lighthouse holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by the Lighthouse, staff, Trustees, volunteers and contractors, referred to herein after as 'staff'.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 (24 hours if an electronic breach) hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within the required time period, it shall be accompanied by reasons for the delay.
2. The notification referred to in paragraph 1 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 be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
 5. The Data Controller shall 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.

Types of Breach

Data protection breaches could be caused by several factors. Several examples are shown below:

- 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;
- Cyber-attack;
- Hacking.

Managing a Data Breach

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

1. The person who discovers/receives a report of a breach must inform The Data Protection Officer or, in their absence, the Management. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Data Protection Officer or nominated person must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system.
3. The Data Protection Officer or nominated person must inform the Chair of Trustees as soon as possible. As a registered Data Controller, it is our responsibility to take the appropriate action and conduct any investigation.
4. The Data Protection Officer or nominated person must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known

GDPR Data Breach Policy

Revised April 2021

or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice should be obtained.

5. The Data Protection Officer or nominated person must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
 - a. Attempting to recover lost equipment.
 - b. Contacting the relevant people / departments / organisations, 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 by the Data Protection Officer.
 - c. 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 the relevant agencies and members of staff informed.
 - g. The person(s) affected by the Data Breach will be contacted and informed as early as feasible.
 - h. In the event of a possible or actual Data Breach that does not require reporting then the details should be recorded and reasons given as to why a report was not made and kept with the GDPR log.

Investigation

In most cases, the next stage would be for the Data Protection Officer to fully investigate the breach. The Data Protection Officer should 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 due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed 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 initial investigation has taken place. The Data Protection Officer should, and may seek expert or legal advice if 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). Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what we are able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the Complaints Procedure). The 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

Review and Evaluation

Once the initial aftermath of the breach is over, the Data Protection Officer 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 put correct these. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Data Protection Officer should ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Data Protection policy and associated procedures, they should discuss this with the Data Protection Officer or the Management.

Review

This policy will be updated as necessary (at least once every two years) to reflect best practice in data management, security, and control to ensure compliance with any changes or amendments made to GDPR or subsequent acts.

Policy Adopted by Management Board: 10/5/18

Policy Last Reviewed on: 15/4/21

Policy Due for Review on: 1st May 2022

Signed Harvey Grahame-Smith

Policy Review frequency: May annually at present