Data Breach Policy

Aims:

This Data Breach / Response procedure sets out the course of action to be followed by all staff and appointed persons at Holy Trinity Boston/ Charity Number 1132300 if a data protection breach takes place or is suspected.

Types of Breach:

Data protection breaches could be caused by a number of factors.

This policy includes, but is not exclusive to:

- Loss or theft of data or the 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

Immediate Containment/Recovery:

In discovery of a data protection breach, the following steps should be followed.

1. The person discovering the potential breach should notify The Church Wardens who are the Data Protection Leads, or their line manager / volunteer coordinator. This report should happen as soon as is practicably possible.
2. The Data Protection Lead should investigate the potential breach asap. Ideally this should be within a few hours, and certainly as soon as is practicably possible. (See Investigation below).
3. Firstly, the Data Protection Lead must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach, including looking for any lost data, restricting physical access to the area where breach is suspected, changing passwords to online systems or shutting down I.T. systems where required.
4. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
5. 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.

Investigation

Data investigations should be documented and should cover:

- The type of 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 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 and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved and this should be reviewed by the Data Protection Leads

Notification:

1. The Data Protection Lead must inform the Parochial Church Council for responsibility and an update; risk assessment and response plan must be discussed at the next meeting.

2. The Data Protection Lead should consider if the Police need to be informed. This is particularly appropriate in the event of suspected theft of data or where the data references sensitive information or data with safeguarding implications.
3. Under GDPR there is a mandatory responsibility to report breaches of data to the ICO*.
(Please note that once the Data Protection Lead has been made aware of your concerns by you personally then your concern will be reported to the ICO with 72 hours)
4. Out of care for your church members, and as a legal obligation, you should report all data breaches to the people (subjects) affected. This should be done as soon as practicably possible, either by an email or posted letter, should outline the details of the breach and the nature of the data contained, provide some advice for how to respond, a method or route of complaint or query and some reassuring language about steps the church have taken to mitigate the effect.
Review and Evaluation:
After a breach has occurred and the appropriate steps have been taken, the response and this policy should be evaluated by the Data Protection Lead and then the findings and any development should be reported to the church council.

Record of Data Protection Breach and subsequent investigation:

Name of Data Protection Lead / Appointed Person:

_____

Date of Breach:

_____

Date of Investigation:

_____

Nature of potential breach: (what has happened?)

_____

_____

_____

When? Where?

_____

What data has been compromised?

_____

What caused the breach? (lost, theft, human error, technical issue etc.?)

_____

Does this include bank and financial details? (if so what?)

_____

Does this include sensitive information? (if so what?)

_____

Is there a safeguarding implication (in particular relation to children or vulnerable adults)?

_____

Is there an immediate cause of concern to someone's safety?

_____

Is there a risk of illegal activity?

_____

Have passwords or key codes been compromised?

_____

What protections are in place?

_____

Has a breach occurred?

_____

Is it ongoing or has the breach ceased?

_____

1. Who is affected?

_____

2. Who should be notified?

3. ICO Notification completed on: [date]_____
4. Church Team Notification completed on: [date] _____
5. Subject of Data Notification completed on: [date] _____
6. SIRO (Trustee) Notification completed on: [date] _____
7. Is there a continuing risk?

_____

8. What steps should be taken to rectify this breach and stop it reoccurring?

1…….
2…….
3……..
4……..

9. Report completed by:

_____

Date: _____

10. Reviewed: [on date] _____

Implementation, Monitoring and Review

· The current policy will be stored, and accessed via the Church Office
· This policy will be reviewed annually and ratified by the PCC.
· Any comments about this policy can be sent to Church Office
· This policy shall be monitored via the PCC and it's representative

Data Breach	**Approved on**
Holy Trinity Parochial Church Council	
Review Date Holy Trinity Parochial Church Council	July 2021

*ICO=Information Commissioners Office