Peterborough Diocesan Board of Finance Data Breach Policy

Policy summary

The Peterborough Diocesan Board of Finance (DBF) uses personal information to carry out their many functions supporting the mission and ministry of the Church of England. Legislation requires and sometimes empowers the DBF to provide goods and services to the wider Church.

The DBF will ensure that they use personal information in line with the expectations and interests of those with whom they come into contact, including their employees, office holders and customers, for the benefit of the Church and wider society and in compliance with data protection legislation.

Data security breaches are increasingly common occurrences whether through human error or via malicious intent. As technology trends change and the creation of data and information grows, breaches can occur in more ways. The DBF needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets, and thus its data subjects as far as possible.

The aim of this policy is to standardise the diocese wide response to any reported data breach incident, and ensure they are appropriately logged and managed in accordance with best practice guidelines [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/]

This DBF wide policy applies to all DBF information, regardless of format, and is applicable to all staff, officers, volunteers, visitors' contractors and data processors acting on behalf of the diocese. It is to be read in conjunction with the DBF Data Protection Policy.

Approval and review

Document Control

Date	Version	Status	Author	Reason for Change	Authorised
01/09/2022	1.0	FINAL	Sue Ratcliffe	Revision of un published 2019 Policy	Andrew Roberts
06/01/2025	1.2	FINAL	Sue Ratcliffe	Review	Andrew Roberts

Contents

1. Introduction

The 'integrity and confidentiality principle of GDPR[1] requires us to ensure we have the appropriate security measures in place to protect the personal data we hold.

The Diocesan Board of Finance will comply with applicable legislation, including:

a. **Data Protection Act 2018**
b. **General Data Protection Regulation 2016**
c. **Human Rights Act 1998, Article 8**
d. **The Common Law Duty of Confidence**
e. **Privacy and Electronic Communications Regulations 2003**
f. **Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011**
g. **In addition, other regulatory requirements and applicable guidance.**

2. Purpose

The purpose of this policy is to standardise the DBF wide response to any reported data breach incident, and to ensure that they are appropriately logged and managed in accordance with best practice guidelines.[Personal data breaches: a guide | ICO]

By adopting a standardised consistent approach to all reported incidents, the Diocese aims to ensure that:

- The reporting, recording and documenting of incidents occurs in a timely manner, and in accordance with legislative requirements.
- The appropriate person/people investigate the incident (s) ensuring a proper and thorough investigation takes place.
- Evidence is gathered, recorded and maintained in a format that will withstand internal and external scrutiny.
- The impact of the data breach is fully understood, is dealt with in a timely manner, and action taken to prevent further breaches/damage occurring.
- The data breach incident becomes an opportunity to implement improvements in policies and procedures.
- The appropriate level of management oversees the incident and the appropriate notifications to external bodies /data subjects.

3. Definition

A personal data breach means 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. A broad definition of a personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data.[2] For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

[1] Also known as the 'security' principle.
[2] Personal data breaches: a guide | ICO

4. Scope

This DBF wide policy applies to all Diocese information, regardless of format, and is applicable to all employees, including agency workers, consultants, contractors and volunteers. It should be read in conjunction with the DBF Data Protection Policy. Failure to comply could result in disciplinary action in accordance with paragraph 35 in the Staff Handbook found here: DBF Staff Handbook - 29.04.24.pdf including dismissal for employees, and termination of contracts with contractors, consultants or agency staff.

5. Responsibilities

5.1. Heads of Department (Directors and similar)
All Heads of Department and those in a 'team manager' position are responsible for developing and encouraging a culture for data protection throughout the organisation. This means they must ensure that staff under their control act in compliance with this policy and assist with investigations as required.

5.2. Information Users
All information users are responsible for reporting actual, suspected, threatened or potential information security incidents. All information users are responsible for assisting with investigations as required, particularly where urgent action is required to prevent further loss/damage.

5.3. Data Protection Officer
The data protection officer will be responsible for overseeing the management of the breach in accordance with this policy and the Data Breach Management Plan [outlined at the appendices]. Suitable delegation may be appropriate in some circumstances.

5.4. Contact Details
All data breach/loss incidents should be reported to the Diocese DPO at sue.ratcliffe@peterborough-diocese.org.uk marked as [!high importance]

6. Data Classification

Data security breaches will vary in impact and risk depending on the content and quantity of the data involved and the type of breach that has occurred. It is important that the DBF is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents should include the appropriate data classification to allow an assessment of risk. Data classification referred to in this policy means the following approved diocese categories.

6.1. Public Data:
Information intended for public use, or information that is already in the public domain. (For example, clergy contact details, or information publicising the work of the Diocese)

6.2. Internal Data:

Information regarding the day-to-day business and operations of the DBF. Primarily intended for staff and student use, although some information may be useful for third parties who work with the DBF (for example internal role information).

6.3. Confidential Data:
Information that should not be in the public domain, and if in the wrong hands, could cause harm to any individual or to the DBF as a whole. (For example, special category information gathered as part of the vocation journey, or bank details belonging to gift aid donors or safeguarding case details).

7. Data Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to sue.ratcliffe@peterborough-diocese.org.uk and marked [**!**high importance] with 'Data Breach' in the subject line. The initial report should be immediately followed up with the data breach reporting form found at **appendix 1.** The report should include full and accurate details of the incident, including who is making the report and what classification of data in involved. If the data security breach involves, or is suspected to involve a breach of our network, then report to the DPO who will in turn report to Optimity our IT provider

The DPO, in collaboration with the reporting officer and / or Optimity, will make an assessment to establish the severity, the risk and therefore response. All data security breaches will be centrally logged by the DPO to ensure appropriate oversight of the types and frequency of conformed incidents for management and reporting purposes.

8. Data Breach Management Plan

The response to any reported data security breach will involve the following four elements.

A. Containment and Recovery.
B. Assessment of Risk.
C. Consideration of Further notification.
D. Evaluation and Response.

A timeline of the incident will be included in the data breach record. It is likely that the level of response will be dictated by the severity of the breach, for example, a failure to use BCC in email correspondence will require a difference level of response to an infection by virus leading to a large scale data loss.

9. Authority

Employees, including agency workers, consultants, contractors , volunteers visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

10. Review

The Assistant Diocesan Secretary will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches

11. References

Information Commissioner

Personal data breaches: a guide | ICO

APPENDIX 1 – Data Breach Reporting form

Email this form to; sue.ratcliffe@peterborough-diocese.org.uk marked as **!**high importance and with 'Data Breach' in the subject bar.

DATA BREACH NOTIFICATION					For DPO
Date and Time the breach was identified and by whom	Description of the data breach	Classification of the data breached; including volume of data involved, and whether it is a confirmed or suspected breach.	Remedial Action Taken; to include whether the breach is contained; or ongoing (and what actions are being taken to recover the data)	Who has been informed of the breach?	Received by: Date/time