SHEFFIELD DIOCESAN BOARD OF FINANCE

DATA BREACH GUIDANCE POLICY

Purpose of Policy

The General Data Protection Regulations (GDPR) places a duty on all organisations, including Sheffield Diocesan Board of Finance (SDBF), to report certain types of personal data breaches to the relevant supervisory authority, normally the Information Commissioners Office (ICO).

If a breach occurs, we must do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to adversely affect individuals' rights and freedoms, then we must also inform those individuals without delay.

The purpose of this policy is to ensure that we have a robust breach detection procedure, which enables us to fully investigate any breaches and report our findings internally, and if necessary to the ICO.

What is a Personal Data Breach?

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 a breach is more than just about losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.

Simply, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative impact on individuals.

Which breaches do we need to notify the Information Commissioners Office (ICO) about?

When a personal data breach has occurred, we need to establish, through our reporting procedures, the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely there will be a risk, we will need to notify the ICO.

When thinking about the risk to an individual's rights and freedoms, we need to consider the following potential consequences of the breach and assess the potential severity of impact: -

- Loss of control over their personal data or limitation of their rights;
- Potential for discrimination;
- Identity theft or fraud;
- Financial loss;
- Unauthorised reversal of pseudonymisation (the processing of personal data in such a way that the data subject can no longer be identified without the use of additional information);
- Damage to reputation;
- Loss of confidentiality; and
- Any other economic or social disadvantage to the natural person concerned.

A data breach can have a range of adverse effects on individuals, which include emotional distress and physical and material damage. We will need to assess this on a case by case basis, considering all of the relevant factors and their potential impacts.

What should I do if a breach occurs?

1. If you become aware of a breach, in the first instance you should try to contain it.
2. You should report the breach immediately to your Line Manager, who will work with you to identify the risks and the potential adverse consequences of the breach;
3. You should gather the facts, including:
    - The date of the breach;
    - The number of people impacted by the breach;
    - The nature of the breach;
    - A description of the breach;
    - The likely consequences of the breach;
    - Any measures you might have already taken or could take to deal with the breach, including any actions that might mitigate against any adverse impacts.
4. You should notify the Data Compliance Officer;
5. You should complete the Personal Data Security Breach Log;
6. After considering all of the facts, and establishing the reason for the breach, the Data Compliance Officer, or nominated deputy, will inform where necessary the ICO, individual data subjects, the SDBF and any other bodies or authorities of the breach.

<u>Notes must be made of any key decisions made and the rationale for these decisions</u>.

In the longer term, having established whether the breach was a result of human error or the result of a systemic failure, we should determine how a reoccurrence can be prevented and put appropriate remedial action in place, for example implementation of better processes, further training or any other corrective step identified.

All breaches should be recorded, regardless of whether or not they need to be reported to the ICO.

For further information or guidance, please contact the Data Compliance Officer (the Diocesan Secretary) on 01709 309100 (DataProtection@sheffield.anglican.org).