North Bradley Baptist Church

North Bradley Baptist Church – Data Breach Policy

In this policy "we" / "us" refers to North Bradley Baptist Church, which is the data controller for your personal data.

This policy should be read in conjunction with our Privacy Notice, which is available at www.nbbc.org.uk or from our Data Protection Officer Phil Taylor (01225 763 583 / dataprotection@nbbc.org.uk).

We hold and process personal data which needs to be protected. Every care is taken to protect the data we hold. We recognise that compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties.

The objective of the Data Breach Policy is to contain any breaches, to minimise the risks associated with the breach and to consider what action is necessary to secure personal data and prevent any further breach.

Types of breach:
An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects. An incident includes, but is not restricted to:

- Loss or theft of personal data or the equipment on which the data is stored; e.g. laptop, memory stick, smartphone, or paper record
- Theft or failure of equipment on which personal data is stored
- Unauthorised use of or access to personal data
- Attempts to gain unauthorised access to personal data
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack

Reporting an incident:
Any person using personal data on behalf of the church is responsible for reporting data breach incidents immediately to the Data Protection Office or in his absence the Trustees. The report should contain the following details:

- Date and time of discovery of breach
- Details of person who discovered the breach
- The nature of the personal data involved
- How many individuals' data is affected

Containment and recovery:
The Data Protection Officer will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. An assessment will be carried out to establish the severity of the breach and the nature of further investigation required. Consideration will be given as to whether the police should be informed. Advice from appropriate experts will be sought if necessary. A suitable course of action will be taken to ensure a resolution to the breach.

Investigation and risk assessment:
An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. A Trustee will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to reoccur. The investigation will take into account the following:

- The type of data involved and its sensitivity
- The protections in place (e.g. encryption)
- What has happened to the data

- Whether the data could be put to illegal or inappropriate use
- Who the data subjects are, how many are involved, and the potential effects on them
- Any wider consequences

Notification:
The Trustees will decide with appropriate advice, who needs to be notified of the breach. Every incident will be assessed on a case by case basis. Consideration will be given to notifying the Information Commissioner if a large number of people are affected or the consequences for the data subjects are very serious. Guidance on when and how to notify the ICO is available on their website: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Notification to the data subjects whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the nature of the data involved. Specific and clear advice will be given on what they can do to protect themselves and what has already been done to mitigate the risks.
The Data Protection Officer will keep a record of all actions taken in respect of the breach.

Evaluation and response:
Once the incident is contained, the Data Protection Officer will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring.

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.