BEDWORTH PARISH

DATA BREACH POLICY
Version 2

Bedworth Parish, as a processor of personal data, must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

What constitutes a breach?

A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A temporary loss of personal data still constitutes a personal data breach.

How might a breach occur?

Data breaches can occur for different reasons, and by employees, parties external to the organisation or computer system errors.

The following are just some examples:

- Loss or theft of data or equipment on which data is stored e.g. a laptop containing personal data is lost or stolen
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error, such as where data has been accidentally deleted or the decryption key has been lost in the case of encrypted data, and the controller cannot restore access, for example from a backup
- Unforeseen circumstances such as a fire or flood or power failure
- Cyber Attack e.g. hacking, phishing, virus, impersonation, encryption by ransomware and malware
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- A temporary loss of data could include, for example, an infection by ransomware (encrypting data until a ransom is paid) leading to a temporary loss of availability until the data could be restored from a backup

What do I need to do?

If you discover or have been alerted to a breach or potential breach you should immediately (and in any event within 48 hours):

1) notify Jayne Taylor-Farren the Data Protection Officer or, in his absence, your line manager who will advise you of the relevant person to notify; and

2) complete the personal data breach log with as much information as possible, a copy of which should be provided to the Data Protection Officer.

The Data Protection Officer (or person acting in his place) should then follow the steps set out in this Data Breach Protocol and in our supplemental guidance for data protection officers/data protection lead.

However the breach has occurred, there are 4 important elements to be considered, and the Data Protection Officer may need your assistance to fulfill their responsibilities in relation to all of these:

A) Containing the breach
B) Assessing risks and impact
C) Reporting the incident (where necessary)
D) Evaluating the response and recovery to prevent future breaches

Step 1 – containing the breach

The following measures may be appropriate in containing a breach:

- **Shut down the system if a computer system error or Cyber-crime event led to the breach – Contact Rev Dave Poultney**
- **Establish whether steps can be taken to recover lost data** (such as remotely disabling a lost laptop or remotely wipe mobile devices) **– Contact Rev Dave Poultney**
- **Reset passwords if they have been compromised – Contact Rev Dave Poultney**
- **Notify the police if criminal activity is suspected and preserve evidence** (such as hacking or theft)

These steps may require internal approval before being taken, or may only be taken by an approved staff member or your line manager. If you are unsure whether you can or should take any of these steps then please contact your line manager and/or the Data Protection Officer (or person acting in his place) immediately to ensure that any necessary steps to contain the breach can be taken as soon as possible.

Step 2 – assessing risks and impact

Ultimately, the Data Protection Officer (or person acting in his place) will make the assessment of the breach and its impact. Even so, any member of staff who discovers or is alerted to a breach has a responsibility to assist the Data Protection Officer wherever possible.

You can do this by thinking about the following points when completing the personal data breach log, as the information will help the Data Protection Officer to decide whether or not to report the breach to the ICO and/or the individual/s affected by the breach:

- **What is the nature/circumstances of the breach?** For example, were papers left on a train, or has someone gained access to the computer system and gained access to personal data?
- **What types of personal data were involved?**
- **How sensitive is the data?** Some data is sensitive because of its personal nature (e.g. client addresses and contact numbers, or information that allows individuals to be easily identified) while other data types are sensitive because of what might happen if it is misused.
- **If data has been lost or stolen, are there any protections in place?** For example, encryption.
- **What has happened to the data?** Has it been stolen or damaged?
- **How many individuals' personal data are affected by the breach?** It is not necessarily the case that bigger risks will accrue from the loss of large amounts of data but it is an important determining factor in the overall risk assessment.
- **Who are the individuals whose data has been breached?** Whether they are employees or customers will to some extent determine the level of risk posed by the breach.
- **What harm can come to those individuals?** Are there risks of identity theft, financial loss or damage to a person's reputation, for example.
- **If individuals' bank details have been lost, consider contacting the bank for advice on anything they can do to help prevent fraudulent use.**

Step 3 – reporting the breach

In certain circumstances it will be necessary to report the breach to the ICO and/or to the individual/s affected by the breach. This decision will ultimately be made by the Data Protection Officer but they may need your input when making this decision.

It is important that you notify the Data Protection Officer of any breach as soon as possible, and provide them with any assistance they require, because:

- Any notifiable data breach has to be reported to the ICO or relevant supervisory authority/ICO within **72 hours** of the organisation becoming aware of the breach.
- If the breach is sufficiently serious to warrant notification to the public, they must be notified without undue delay.
- If the Data Protection Officer fails to notify either the ICO and/or the data subjects as appropriate, then we may face a fine of up to €10,000,000 or up to 2% of the total worldwide annual turnover of the organisation. It is therefore vital to provide the Data Protection Officer with all the assistance they may require.

Step 4 – evaluating the response and recovery to prevent future breaches

Following any breach the Data Protection Officer will identify where improvements can be made to ensure that the organisation's existing procedures do not lead to any further breaches.

Please provide them with any assistance they require in ensuring that our security measures and data protection policies are satisfactory to protect the personal data we hold.

Useful telephone numbers:

Information Commissioners Office (ICO)	0303 123 1113
Jayne Taylor-Farren - Data Protection Officer	finance@bedworthparish.org
Rev Dave Poultney	02476 102141

If you are at all unsure of the steps that you need to take in the event of a data breach, or if you believe a data breach may have occurred, then please contact your Data Protection Officer.