Widecombe-in-the-Moor Parish Council

DATA BREACH RESPONSE PLAN

1. A data breach of any size is a crisis management situation, which could put an entire council at risk. Data security is not an IT issue, it is an organisational risk, and breach response should involve people from a number of roles across the council.

2. A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

   Examples of personal data breaches and steps to avoid them include:

   - Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.
   - The wrong people being copied in to emails and attachments. Use BCC (Blind Carbon Copy) where necessary.
   - Lost memory sticks which contain unencrypted personal data. The council should put protocols in place for memory stick usage.
   - Malware (IT) attach. Ensure up to date anti-virus software is in place.
   - Equipment theft. Check security provisions.
   - Loss of personal data which is unencrypted.

3. The Clerk should be notified if there is a data breach and he/she will inform all Parish Councillors. When a personal data breach has occurred, the Council needs to establish the likelihood and severity of the resulting risk to people's rights and freedoms. In assessing this risk, it is important to focus on the potential negative consequences for individuals.

4. If it is likely that there will be a risk, e.g. the data breach could lead to identity theft, financial loss or physical or emotional harm, then the Council must notify the ICO and the data subject as soon as possible and within 72 hours of its discovery.

5. If it is unlikely that there will be a risk, e.g. the Council sent an email to the wrong person and there was nothing sensitive in the email, then the Council does not have to report it to the ICO but it should inform the data subjects.

6. If the Council decides not to report the breach, it needs to justify this decision and it should be documented.

7. Data breaches will be recorded using the ICO's online system: https://ico.org.uk/for-organisations/reporta-breach/ and the following information should be provided:

   - The potential scope and cause of the breach
   - Mitigation actions the council plans to take
   - Details of how the council plans to address the problem.

8. In line with the accountability requirements, all data breaches must be recorded by the parish council along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data.

9. If anyone (including a third party) suspects that a data breach has occurred, details of the alleged breach should be submitted immediately in writing to the Clerk.

Adopted by Widecombe-in-the-Moor Parish Council on 5 July 2018