

1. What is a 'personal data breach'?

- 1.1. 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.
- 1.2. Personal data breaches can include:
 - 1.2.1. access by an unauthorised third party;
 - 1.2.2. deliberate or accidental action (or inaction) by a controller or processor;
 - 1.2.3. sending personal data to an incorrect recipient;
 - 1.2.4. computing devices containing personal data being lost or stolen;
 - 1.2.5. alteration of personal data without permission; and
 - 1.2.6. loss of availability of personal data.
- 1.3. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, 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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
- 1.4. Pencombe Group Parish Council ("the Council") has a responsibility to ensure that personal data is kept and used securely. If anything goes wrong and data is lost, stolen, misused, sent to the wrong address or inappropriately accessed or released, we have a responsibility to put things right.

2. What happens if there is a data breach?

- 2.1. When a personal data breach has occurred, The Council will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then the Council will notify the Information Commissioner's Office (ICO); if it's unlikely then it won't be reported.
- 2.2. If the breach is not reported to the ICO the Council will still document the breach to be able to justify the decision.

3. Reporting a data breach

- 3.1. The Council must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it.
- 3.2. When reporting a breach, the following information must be provided:

- 3.2.1. A description of the nature of the personal data breach including, where possible:
 - 3.2.1.1. the categories and approximate number of individuals concerned; and
 - 3.2.1.2. the categories and approximate number of personal data records concerned.
- 3.2.2. The name and contact details of the contact point where more information can be obtained.
- 3.2.3. A description of the likely consequences of the personal data breach.
- 3.2.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

4. Informing individuals about a breach

- 4.1. If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will inform those directly and without undue delay, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.
- 4.2. If the Council decides not to inform individuals it will still notify the ICO, unless it can be demonstrated that the breach is unlikely to result in a risk to rights and freedoms.
- 4.3. When informing individuals of a data breach the Council will describe, in clear and plain language:
 - 4.3.1. The nature of the personal data breach.
 - 4.3.2. The name and contact details of the contact point where more information can be obtained.
 - 4.3.3. A description of the likely consequences of the personal data breach.
 - 4.3.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

5. Failure to notify

- 5.1. Failing to notify a breach when required to do so can result in a significant fine up to €10m.

This Personal Data Breach Policy was adopted by the Parish Council at a meeting of the Council held on:

26th June 2018
