Wokingham Without Parish Council

Data Breach Policy

Version 1.1

Adoption Date: 04/03/2019 Minute Reference: 18/893 Next Review Date: March 2021

Introduction and scope

1. The parish council holds a large amount of information in a variety of formats stored on computers, in written documents (including leases), printed documents and images in the form of photographs. This includes personal and sensitive personal data, and also non-personal information which may be sensitive or commercially confidential
2. The parish council has legal responsibilities to safeguard information in its control. Care should be taken to protect information, to ensure its integrity and to protect it from loss, theft or unauthorised access.
3. In the event of an information security incident (also referred to as a 'data breach'), it is vital that appropriate action is taken to minimise associated risks. A risk analysis should be performed, factors which need to be considered are:
    a. The number of individuals affected
    b. The type of data involved
    c. The likely impact

Data breaches

1. A data breach is an event whereby data held by the Parish Council, in any format, is compromised by being lost, destroyed, altered, copied, transmitted, stolen, used or accessed unlawfully or by unauthorised individuals whether accidentally or on purpose. Some examples of data breaches include:
    - Unauthorised access to data – e.g. emails and attachments being sent to the wrong person, public posting of confidential information online or incorrect sharing of documents
    - Loss or theft of equipment on which data is stored
    - Malware (IT) attack or data maliciously obtained

2. Understanding the issues that arise in a breach situation, and recording 'near misses' to identify vulnerabilities where the council considers there is a high likelihood of an actual incident occurring are essential to effective breach response.

The data breach response plan

1. All data breaches should be reported to the Clerk, and Chairman
2. The report should include full and accurate details of the incident, including:
    - Who is reporting
    - What type of data is involved (personal data, sensitive personal data etc)
    - How the data was held (e.g. electronic format, paper)
    - If the data relates to people and if so, how many people are involved
3. The Clerk and Chairman will consider the report, and where appropriate, instigate a Response Team (The Parish Clerk, Chairman plus two other councillors[1]). The Response Team will be responsible for investigating the circumstances and effect of the breach. Where practicable, the investigation will be started within 24 hours of the breach being discovered. The Response Team will appoint a Team Leader.

[1] Given the short timeframe in which to report an incident to the ICO, the Response Team membership will be dictated by availability

4. The Response Team Leader is responsible for formally documenting the incident and associated response.

Containment and recovery

1. The Parish Council will determine the appropriate course of action and the required resources needed to limit the impact of the breach. For instance, this may require alerting relevant groups, organisations, parishioners, contractors or suppliers, changing access codes or locks or shutting down critical equipment.
2. Appropriate steps will be taken to recover data losses. This might entail using backup mechanisms to restore compromised or stolen data and changing compromised passwords.
3. For incidents that involved a suspected or actual criminal offence, all efforts will be made to preserve evidence integrity.

Escalation and Notification

1. The Response Team is responsible for the initial assessment of an incident's severity based on the scope, scale and risk of the incident. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals
2. If a personal data breach has occurred of sufficient scale, the Response Team will notify the Information Commissioners Office (ICO) within the prescribed statutory time limits (currently within 72 hours of discovery of the breach) . The Clerk will manage all communication between the Parish Council and the ICO.
3. Notice of the breach will also be made to affected individuals to allow them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the Response Team. Liaison with the Police or other authorities may be required for serious events.
4. In the event that the Response Team determine that the incident does not merit reporting to the ICO, the justification for this reason must be recorded.

Reporting to the ICO

1. Breaches should be reported to the ICO on 0303 123 1113
2. The report to the ICO shall at least:
    - Describe the nature of the personal data breach including where possible, the categories (e.g. members of the public, volunteers or Councillors) and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    - Communicate the name and contact details of the Clerk or other contact point where more information can be obtained;
    - Describe the likely consequences of the personal data breach;
    - Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects e.g. advising affected members of the public to change e-mail or banking passwords.

Other sources of support

The Council may need external assistance from:

- WWPC's IT support provider: SIBIT Tel. 01344 769 090
- Providers of the relevant operating system e.g. Microsoft for Windows PC breaches.
- The police for theft of documents. Call 101 and ask for Thames Valley Police.
- The ICO 0303 123 1113

Review

1. Once the incident is contained, a thorough review of the incident will be undertaken by the Response Team to establish the cause of the incident, the effectiveness of the response and to identify areas that require improvement.
2. This review will be presented to the full council
3. Recommended changes to systems, procedures and policies that are agreed by the council will be documented and implemented as soon as possible thereafter.