Rooksdown Parish Council

Data Breach Response Procedure

V1 March 2019 as approved

1 Purpose

This document specifies the procedure that must be followed by councillors and council employees in the event of a data breach.

2 What is a breach?

2.1 Definition

A 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.

2.2 Examples

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- and loss of availability of personal data.

3 Dealing with an incident

3.1 Report the incident

Any person discovering an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, shall:

- Report the incident in an email to the chairman - or in his absence the vice chairman - and the clerk
- Telephone the chairman - or in his absence the vice chairman - and the clerk.

3.2 Managing the incident

Responsibility for managing the incident (as the **incident manager**) will be taken by the clerk, or in their absence, the chairman or vice chairman.

On receipt of an incident report the incident manager shall:

- Note the time, date and nature of incident including a description and as much detail as appropriate.
- Ensure the protection of any evidence and that a documented chain of evidence is maintained.
- Assess the breach as detailed below:
    - If a **notifiable breach**:
        - Notify the Information Commissioners Office (ICO)
        - Notify the affected individuals

- If necessary, liaise with any other authorities, individuals and the media.

- Keep a note of all communications together with their date, time, who has been communicated with, and what the content and nature of communication was.

3.3 Incident Response Plan

3.3.1 Assess the breach

The following must be considered:

- The categories and approximate number of individuals involved
- The categories and amount personal data involved
- The likelihood and impact of the breach on the rights and freedoms of individuals.
- To help assess the risks refer to the Information Commissioner Office (ICO) website:
  - https://ico.org.uk/for-organisations/report-a-breach/
- If there is a significant risk to the rights and freedoms of individuals, the breach must be classified as a **notifiable breach**.

3.3.2 Notifiable breach

If the incident is a **notifiable breach** the following actions must be taken:

- Report the breach to the Information Commissioners Office (ICO) within 72 hours of becoming aware of the incident, even if all details are not yet available
  - Details of how to report a breach can be found at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- Within 48 hours the affected individuals must be informed by telephone, letter or email about the incident as there may be a need for them to take actions to mitigate immediate risk of damage to them. The individuals must be told in clear and plain language:
  - the nature of the personal data breach
  - A description of the likely consequences of the personal data breach
  - 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
  - The name and contact details (clerk/chairman) from where more information can be obtained.

3.3.3 Non-notifiable breach

If the incident is not deemed to be notifiable, the incident manager shall make a written record of the risk assessment process, and outcome, including a clear statement as to why the incident is non-notifiable.

4 Incident Review:

- The clerk will place an item on the agenda of the next appropriate Council meeting to review the incident.
- If the review is likely to result in discussion of confidential data or procedures the council shall consider excluding the press and public from the meeting during that discussion.
- At that meeting the council should determine if there are any further actions that need to be assigned or completed as a result of the incident.
- The council may decide to refer further actions and to a committee, working group or external parties.
- It should be noted that this final stage of the incident may require a review of this policy document.

MARTIN WHITTAKER

Clerk to Rooksdown Parish Council

Rooksdown Community Centre
Park Prewett Road, Basingstoke RG24 9XA

07928 129122