Deeping Gate Parish Council

Data Breach Procedure

To be adopted, 10th March 2026

Minute: 26.27.2.c

1. What is Data Breach?

A breach is a security incident leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data. Examples include:

- Loss of a laptop, mobile phone, or unencrypted USB stick
- Sending personal data (e.g. an email or letter) to the wrong recipient
- Theft of paper records or unauthorised access to the Council's cloud storage.
- Cyber attack of "phishing" incident where data is compromised.

All data held by the Council, including paper, electronic and cloud storage, falls under this procedure.

2. Immediate Action (the first 24 hours)

Any councillor or employee who becomes aware of a suspected or confirmed breach must:

1. Inform the Clerk immediately (or the Chair if the Clerk is unavailable)
2. Contain the breach if possible (e.g., ask a recipient to delete a misdirected email).
3. Preserve evidence (e.g. do not delete logs of emails related to the incident).

3. Assessment and Logging

The Clerk will:

- Record the incident in the Council's Breach Log, regardless of whether it needs to be reported.
- Assess risk to individuals (e.g., could this lead to identity theft, financial loss, or loss of confidentiality?)
- Determine if the breach is "reportable" under UK GDPR.

4. Reporting to ICO

- If the breach presents a risk to the rights and freedoms of individuals, the Clerk must notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.
- If the breach is likely to result in a high risk to individuals, they must also be informed directly, without undue delay.

5. Responsibilities

The Council has appointed The Clerk as the person responsible for data protection compliance.

The Clerk is responsible for managing the investigation, notifying the ICO, and updating the Council's security measures following a breach.

Councillors are responsible for ensuring any Council-related data held on personal devices is reported if that device is lost or stolen.

6. Post-Breach Review

Following any breach, the Council will:

- Investigate the cause of the breach.
- Review and update technical or organizational measures (e.g., staff training, new password policies).
- Report the outcome of the review to the next Council meeting (in an exempt session if necessary to protect security).

7. Individual Rights

Individuals may exercise their rights under UK GDPR, as set out in the Council's Data Protection Policy, including access, rectification and erasure.

8. Technical and Organisational Measures

The Council will implement appropriate technical and organisational measures to protect personal data, including:

- Secure email and password protection
- Restricted access to sensitive data
- Locked storage for paper records
- Secure disposal of confidential waste

9. Data Retention

The Council will retain personal data only for as long as necessary to fulfil its purpose or comply with legal obligations.

Retention periods will be set out in the Council's Document Retention Schedule.

The Council will provide clear Privacy Notices explaining:

- What data is collected
- Why it is collected
- Lawful basis
- How long it is kept
- Individual rights

Separate Privacy Notices may apply for:

- Employees
- Councillors
- Members of the public
- Website users

Document History and Review			
Version	**Adoption date**	**Minute Ref.**	**Notes**
1.0	10th March 2026	26.27.2.c	First adoption

Next scheduled review: March 2027