Nash Parish Council – Data Breach Procedure

1. Purpose

This procedure sets out how the Council will respond to any personal data breach to ensure:

- swift containment and recovery
- assessment of risk
- compliance with UK GDPR and the Data Protection Act 2018
- appropriate reporting to the Information Commissioner's Office (ICO) and affected individuals

All councillors, staff, contractors and volunteers must follow this procedure.

2. What is a Personal Data Breach?

A personal data breach is **any** accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:

- lost or stolen laptops, USB drives, or paperwork
- sending personal data to the wrong recipient
- unauthorised access to systems or email accounts
- ransomware or cyber-attack
- accidental deletion or alteration of personal data
- publishing personal information in error

3. Responsibilities

- **All councillors/staff**: Must immediately report suspected breaches.
- **Clerk / Responsible Finance Officer (RFO)**: Usually acts as the first point of response and provides advice, evaluates risk, and determines if the breach must be reported to the ICO.

Contact details

- Clerk & RFO: Kelly Harris, clerk@nash-bucks-pc.gov.uk / 07793 131810

4. Step-by-Step Procedure

Step 1: Identify and Report Immediately

As soon as a breach or suspected breach is discovered:

- Report it immediately to the Clerk.
- Prompt reporting is essential—UK GDPR requires serious breaches to be assessed and possibly reported within 72 hours.

Step 2: Contain the Breach

The Clerk will act to limit the damage. Actions may include:

- Recovering lost equipment or documents
- Changing passwords / revoking access
- Shutting down compromised accounts or systems
- Contacting IT support
- Stopping further transmission or publication of data

Step 3: Assess the Risk

The Clerk must quickly assess:

- **What data is involved?** (name, address, financial data, sensitive data, etc.)
- **How many individuals are affected?**
- **Could the breach cause harm?** e.g. identity theft, financial loss, distress, discrimination, reputational damage
- **Has the data been recovered or securely contained?**
- **Who accessed or might access it?**

Use the ICO's "Personal Data Breach Guidance" for risk assessment.

Step 4: Decide Whether to Report to the ICO

A breach must be reported to the ICO if it is likely to result in a risk to the rights and freedoms of individuals.

Examples of breaches likely to require reporting:

- Any compromise involving sensitive (special category) data
- Large-scale breaches or widespread exposure
- Disclosure of financial data, ID documents, or vulnerable individuals' details

- Cyberattacks involving system access

The ICO must be notified:

- Within 72 hours of becoming aware of the breach
- Using the ICO's online reporting tool

If the Council decides not to report:

- The decision and reasoning must be documented.

Step 5: Notify Affected Individuals (if required)

If a breach is likely to result in a high risk to individuals, they must be informed without delay.

The notification should include:

- A description of the breach
- What personal data was involved
- Likely consequences
- What the Council is doing to address it
- Advice on what the individual can do to protect themselves

Examples where notification is normally required:

- Data published online
- Unencrypted laptop or USB containing personal data lost or stolen
- Sensitive data accessed by an unauthorised person

Step 6: Record the Breach

All breaches—reported or not—must be logged, including:

- date and time of breach
- summary of what happened
- categories and volume of data involved
- actions taken
- risk assessment
- decision on reporting to ICO & individuals
- follow-up measures

Records must be kept for at least 6 years.

Step 7: Review and Prevent Future Breaches

After the incident is closed:

- Review the cause of the breach
- Identify improvements (training, updated procedures, technical changes, encryption, etc.)
- Update policies where necessary
- Discuss lessons learned at the next appropriate Council meeting (excluding confidential details)

5. Examples of Immediate Actions

- Email sent to wrong recipient → ask recipient to delete; confirm deletion
- Lost paper file → trace last known location
- Cyber incident → isolate device, change passwords, contact IT support
- Website error publishing personal data → remove content immediately, clear caches.

6. Training and Awareness

All councillors, volunteers, and staff with access to personal data should:

- Receive data protection and breach-response training
- Know how to recognise and report a suspected breach

Regular refresher training is recommended.

7. Policy Review

This procedure will be reviewed every two years, or sooner if legislation, guidance, or the Council's operations change.

Adopted: 28th January 2026