Sturminster Newton Town Council

Data Breach Procedure (UK GDPR)

This procedure sets out how Sturminster Newton Town Council ("the Council") will identify, record, assess, and report any personal data breach in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Summary: Data Breach Response Flow

Step	Action	Responsibility	Timescale
1. Detect	Identify or suspect a personal data breach	Any councillor, employee, or contractor	Immediately
2. Report	Notify the Town Clerk (or Mayor if it involves the Clerk)	Person identifying the breach	Immediately
3. Assess	Log, investigate, and assess risk to individuals	Town Clerk (Data Protection Lead)	Within 24 hours
4. Notify	Report to ICO (if risk identified) and affected individuals	Town Clerk	Within 72 hours
5. Review	Record, learn, and update policies or training	Town Clerk and Council	Within 1 month

1. Purpose
This procedure ensures that all personal data breaches are identified, assessed, reported, and recorded promptly and in compliance with the UK GDPR and Data Protection Act 2018.

2. Definition of a Data Breach
A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:

- Sending personal data to the wrong recipient
- Loss or theft of devices or paper records
- Accidental deletion or alteration of records
- Unauthorised access (e.g. hacking or misuse of passwords)
- Verbal disclosure of confidential information

3. Reporting a Suspected Breach
Any councillor, employee, or contractor who becomes aware of a potential or actual data breach must report it immediately to the Town Clerk (Data Protection Lead).

If the breach involves the Town Clerk, it should be reported to the Mayor or Deputy Mayor.

4. Initial Assessment
The Town Clerk will log the breach and carry out an initial assessment to determine:

- The nature of the data involved (personal, special category, confidential, etc.)
- How many people are affected and the potential harm
- Whether the breach is likely to result in a risk to individuals' rights and freedoms
- What immediate containment or mitigation actions are required

5. Notification to the ICO
If the breach is likely to result in a risk to individuals, the Town Clerk will report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

The notification will include:

- A description of the nature of the breach
- Categories and number of individuals and records affected
- Likely consequences of the breach
- Measures taken or proposed to address it

If the 72-hour deadline cannot be met, the reason for delay must be documented.

6. Notification to Individuals
If the breach is likely to result in a high risk to individuals, the affected people will be informed without undue delay.

The notification will describe the nature of the breach, its likely consequences, and advice on steps they can take to protect themselves.

7. Containment and Recovery
The Town Clerk will ensure all immediate containment actions are taken to limit the scope and impact of the breach.

This may include isolating systems, changing passwords, restoring backups, or retrieving disclosed data where possible.

8. Recording and Investigation

All breaches, whether reportable or not, must be logged in the Data Breach Register, including:

- Date, time, and nature of the breach
- How it was discovered
- Individuals or data affected
- Actions taken and decisions made
- Any reports to the ICO or individuals

The Town Clerk will carry out an investigation and prepare a brief report for the Council if appropriate.

9. Review and Learning

After each breach, the Town Clerk will review:

- The cause of the breach
- The effectiveness of the response
- Any improvements needed to policies, training, or systems

10. Training and Awareness

All councillors, staff, and volunteers will receive data protection training and guidance on identifying and reporting potential breaches promptly.

The Council is committed to protecting personal data and ensuring all breaches are handled promptly, fairly, and transparently.

Adopted October 2025

Next Review Due: October 2027