DATA BREACH POLICY

(Compliant with UK GDPR & Data Protection Act 2018)
Version: 1.0
Status: Draft for Council Adoption
Review cycle: Annual or following an incident

---

1. Purpose of this Policy

The purpose of this policy is to ensure that Arlesey Town Council responds promptly, effectively and lawfully to any personal data breach, in accordance with:

- **UK GDPR requirements for breach detection, reporting and investigation**
- **Data Protection Act 2018 obligations**
- **ICO guidance on personal data breaches** (legal requirement to report within 72 hours of becoming aware)

This policy applies to all councillors, officers, volunteers and contractors handling personal data on behalf of the Council.

2. Definition of a Personal Data Breach

A personal data breach is *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data"* (UK GDPR).

Examples include:

- Losing council laptops, USB sticks, mobile phones
- Sending information to the wrong person (email or post)
- Unauthorised access to Council systems
- Cyber-attacks (phishing, malware, hacking)
- Accidental deletion or alteration of records
- Disclosing personal data in minutes, agendas or public documents
- Failure to redact information before publishing online

3. Roles and Responsibilities

Clerk (Data Controller's Representative)

- Leads breach investigation
- Assesses severity and risk
- Determines whether the ICO must be notified
- Maintains the Data Breach Register
- Reports outcomes to Council

All Staff & Councillors

- MUST report any suspected breach **immediately** (within 2 hours of becoming aware)
- MUST NOT attempt to hide, delay, delete or “fix quietly”
- MUST cooperate fully with investigations

Council (as Data Controller)

- Ensures policies and training are in place
- Reviews breaches and instructs corrective action

4. Identifying a Personal Data Breach

A breach may be:

A. Confidentiality breach

Unauthorised disclosure or access (e.g. email sent to wrong address)

B. Integrity breach

Unauthorised alteration of data

C. Availability breach

Data being lost, deleted or destroyed

Incidents may involve electronic systems, paper records, CCTV, website content, or mobile devices.

5. Reporting a Suspected Breach (Mandatory)

Any councillor, staff member, contractor or volunteer **must report** a breach immediately to:

Email: clerk@arlesey-tc.gov.uk
Telephone: 01462 733722

Reports must include:

- What happened
- When it happened
- What personal data is involved
- Who is affected
- Whether the data was encrypted/protected
- Any actions already taken

6. Initial Assessment (within 2 hours of becoming aware)

The Clerk will:

1. Record the incident in the **Data Breach Register**
2. Secure systems and prevent further loss
3. Identify the personal data involved
4. Identify categories and number of individuals affected
5. Assess whether the breach poses a **risk to rights and freedoms**

If risk is identified, the Council may be legally required to:

- Notify the ICO within **72 hours of awareness**
- Notify affected individuals **without undue delay**

7. ICO Notification (within 72 hours)

Under UK GDPR, the Town Council MUST report a breach to the ICO **if** it is likely to result in:

- Financial loss
- Identity theft
- Distress or anxiety
- Discrimination
- Reputational damage
- Exposure of vulnerable individuals

ICO reporting is done via the official breach reporting tool on their website.

The Clerk will prepare:

- Description of the breach
- Types and volume of data
- Number of individuals affected
- Likely consequences
- Actions taken or proposed
- Contact details for follow-up

Failure to report a notifiable breach can result in regulatory action.

8. Communicating with Affected Individuals

If the breach is likely to result in **high risk**, the Council MUST communicate with affected individuals promptly.

Notification will include:

- What happened
- What information was involved
- What the Council has done
- What the individual can do to protect themselves

- Clerk contact details
- ICO rights information

Where contact details are missing, the Council may publish a public notice.

9. Investigation & Corrective Actions

The Clerk will complete a full investigation within **14 days** unless extended for valid reasons.

The investigation will identify:

- Cause of the breach
- Weaknesses in processes or systems
- Training needs
- Whether disciplinary or procedural action is required
- Long-term prevention measures

The Clerk will produce a written report to the Full Council or Personnel Committee (as appropriate).

10. Record Keeping

The Council must maintain an internal **Data Breach Register**, documenting:

- Date of breach
- Type of breach
- Personal data categories
- Individuals affected
- Whether ICO was notified
- Decision-making process
- Actions taken or planned
- Review outcomes

The ICO may request access to this register at any time as part of regulatory oversight.

11. Preventative Measures

Arlesey Town Council will meet its UK GDPR obligations by ensuring:

- Regular staff and councillor training
- Secure password and device management
- Lockable storage for paper files
- Encryption for portable devices
- Regular backups
- Redaction procedures for agendas/minutes
- Secure disposal of confidential waste
- Data Protection Impact Assessments (DPIAs) where appropriate
- Annual policy reviews

12. Data Breach Policy Review

This policy will be reviewed:

- Annually
- Following a data breach
- Following changes to ICO guidance
- Following legislative changes

The Clerk is responsible for initiating the review. Full Council must approve any revisions.

Approved by: Arlesey Town Council
Minute reference: 25/189.14
Adopted on: 24th March 2026
Next review: March 2027