



Data Breach Policy

1. Introduction

Upton Parish Council ("the Council") is committed to safeguarding the personal data it holds and processes. In the event of a data breach, the Council will act promptly to mitigate the impact, protect individuals' rights, and comply with its legal obligations under the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA).

This policy outlines the steps to be taken in the event of a data breach.

2. Definition of a Data Breach

A data breach is defined as a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches resulting from both accidental and deliberate causes.

3. Types of Data Breaches

Data breaches may include, but are not limited to:

- **Confidentiality Breach:** Unauthorised access or disclosure of personal data.
- **Integrity Breach:** Unauthorised alteration of personal data.
- **Availability Breach:** Loss or destruction of personal data.

4. Immediate Response to a Data Breach

Containment and Recovery

- Identify and contain the breach to prevent further unauthorised access or damage.
- Recover any compromised data and secure systems involved.
- Determine the cause of the breach and take steps to prevent recurrence.

Assessment of Risk

- Assess potential risks to data subjects as a result of the breach.
- Evaluate severity and scope, including the types of data involved, the number of individuals affected, and potential harm.

- Consider the Council’s lawful basis for processing, including recognised legitimate interests introduced under the DUAA, where applicable.

Notification Requirements

- Notify the Information Commissioner’s Office (ICO) within 72 hours of becoming aware of the breach, where it poses a risk to individuals' rights and freedoms.
- Follow the ICO’s “report early, update later” principle, submitting initial breach details promptly even where information is incomplete.
- Inform affected data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
- Provide clear information to affected individuals about the nature of the breach, likely consequences, and mitigation steps taken.

5. Reporting a Data Breach

All data breaches must be reported immediately to the Data Protection Officer (DPO) or designated responsible person within the Council. Reports should include:

- A description of the breach
- The types of data involved
- The number of data subjects affected
- Possible consequences
- Steps taken or proposed to mitigate harm

The Council must also document whether only “reasonable and proportionate” steps were possible in responding to any associated Data Subject Access Requests (DSARs), in line with DUAA clarifications.

6. Investigation and Documentation

The DPO or designated person will lead the investigation, documenting:

- Nature and cause of the breach
- Actions taken to contain and recover the data
- Risk assessments conducted
- Notifications made to the ICO and affected individuals
- Recommendations and follow-up actions
- Evidence of timely decision-making and adherence to ICO expectations

- Assessment of any automated decision-making processes involved and application of DUAA safeguards, where relevant

7. Review and Improvement

Following a breach, the Council will:

- Review and analyse the incident to identify lessons learned
- Update procedures and policies to prevent recurrence
- Provide staff training on data protection and breach response, reflecting DUAA requirements and current ICO priorities on transparency and accountability

8. Data Breach Log

The Council maintains a Data Breach Log that records:

- Date of breach
- Date discovered
- Description of breach
- Individuals affected
- Categories of data involved
- Impact assessment
- Actions taken
- Notifications issued
- Follow-up measures

The log will also record:

- Any provisional breach information submitted early to the ICO
- Use of DUAA “stop-the-clock” provisions for DSARs where clarification was required

9. Contact Information

For questions or concerns about this policy or the Council’s data protection practices, please contact:

The Clerk

clerk@upton-pc.gov.uk

Adopted: January 2025

Reviewed: March 2026