DURRINGTON TOWN COUNCIL

Data Breach Policy

---

1. **Introduction**
   Durrington Town Council is committed to protecting personal data. A data breach is any event where personal data is lost, accessed without permission, or accidentally disclosed. Breaches can harm individuals, damage the council's reputation, or lead to legal penalties.

---

2. **Who this applies to**
   This policy applies to all councillors, staff, volunteers, and contractors working for Durrington Town Council.

---

3. **What counts as a data breach**
   Examples include:

- Loss or theft of data or devices (laptops, USBs, tablets, paper records)
- Hacking, malware, ransomware, or phishing attacks
- Sending personal information to the wrong person
- Human error, such as leaving files unlocked or misplacing equipment
- Equipment failure or natural disasters (fire, flood)

Near misses are incidents where a breach was avoided, e.g., an email sent to the wrong person but bounced back.

---

4. **Reporting a breach**
   All staff must report suspected or actual breaches immediately to the Town Clerk or, if unavailable, the Deputy Clerk:

Town Clerk / Deputy Clerk
Durrington Town Council, Council Office, Village Hall, High Street, Durrington, Wilts SP4 8AD.
Tel: 01980 654772
Email: clerk@durringtontowncouncil.gov.uk /enquiries@durringtontowncouncil.gov.uk

The Town Clerk or Deputy Clerk will assess the breach, decide whether to notify affected people, and report to the ICO if required.

---

5. **Timetable for handling breaches**

Action	Responsible	Timeline
Identify & contain breach	Town Clerk / Deputy Clerk	Immediately / same day
Initial assessment	Town Clerk / Deputy Clerk	Within 24 hours
Notify ICO (if high risk)	Town Clerk / Deputy Clerk	Within 72 hours
Notify affected individuals	Town Clerk / Deputy Clerk	Without undue delay
Review & lessons learned	Town Clerk / Deputy Clerk	Within 1–2 weeks

---

6. **Handling a breach**

   The Town Clerk or Deputy Clerk will follow these steps:

   Identify – Check what happened and who/what is affected.
   Contain – Stop the breach from getting worse.
   Eradicate – Remove the cause (e.g., malware, lost device).
   Recover – Restore systems and data from backup if needed.
   Review – Learn from the incident and improve policies, training, or security measures.

All breaches should be handled as quickly as possible, ideally within 24 hours.

---

8. **Monitoring and compliance**

- Town Clerk (or Deputy Clerk in absence) monitors compliance.
- Intentional breaches or failure to follow policy may result in disciplinary action.
- Records of breaches and actions will be kept for at least 3 years.

---

9. **Review**

- Reviewed annually or sooner if laws or risks change.
- Next review: February 2027.

---

10. References

- Data Protection Act 2018 – https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- UK GDPR guidance – https://ico.org.uk/for-organisations/guide-to-data-protection/uk-gdpr/
- Reporting a breach – https://ico.org.uk/for-organisations/report-a-breach/

Appendix 1 – Data Breach Report Form

1. **Incident Details**

- Date/time of incident:

- Location:

- Who reported it:

- Description of incident:

2. **Recovery Actions**

- Steps taken to limit/recover data:

- Support given to affected individuals:

3. **Affected Individuals**

- Number affected:

- Were they informed? (Yes/No):

- Consequences or risks:

Appendix 2 – Breach Management Record

Incident number:

Severity: High / Medium / Low

Town Clerk / Deputy Clerk handling incident:

Summary of breach:

Steps Taken:

1. Identify

2. Contain

3. Eradicate

4. Recover

5. Review / Learn

Decision to report to ICO: Yes / No

Decision to inform affected people: Yes / No

Signed: _____ Date: _____