Midgham Parish Council

Information Technology (IT), Digital & Data Compliance Policy

---

1. Introduction

1.1 Midgham Parish Council ("the Council") recognises that the effective use of information technology and the secure handling of data are essential to its operations.

1.2 This policy sets out the framework for the lawful, secure, and appropriate use of IT systems and the management of Council data.

1.3 This policy applies to all councillors, employees, contractors and any individual acting on behalf of the Council.

---

2. Legislative Framework

2.1 This policy supports compliance with the following legislation and guidance:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Equality Act 2010
- The Joint Panel on Accountability and Governance Practitioners' Guide

---

3. Scope

3.1 This policy applies to:

- All devices used for Council business (including personal devices)
- All Council data, regardless of where it is stored
- All systems, software, email accounts and digital services used by the Council

3.2 The Council does not operate from a fixed office location. Accordingly, this policy applies to all locations from which Council business is conducted.

---

4. Roles and Responsibilities

4.1 The Council shall:

- Approve and review this policy annually
- Ensure appropriate governance and risk management arrangements are in place

4.2 The Clerk (Responsible Financial Officer where applicable) shall:

- Ensure day-to-day compliance with this policy
- Maintain oversight of systems, access, and incidents
- Act as the primary point of contact for IT and data matters

4.3 The Data Protection Officer shall:

- Provide advice on data protection compliance
- Support the management of data breaches and privacy matters

4.4 All users shall:

- Comply with this policy
- Protect Council data
- Report any incidents or concerns without delay

---

5. Acceptable Use

5.1 IT systems and devices used for Council business must be used responsibly, lawfully, and in a manner consistent with the Council's duties.

5.2 Users must not:

- Access, store, or transmit unlawful or inappropriate material
- Introduce security risks through unsafe or unauthorised software or services

---

6. Use of Personal Devices (BYOD)

6.1 Where Council-issued devices are not provided, personal devices may be used for Council business, subject to compliance with this policy.

6.2 All devices used for Council purposes must meet the following minimum standards:

- Protected by password, PIN, or biometric authentication
- Configured to lock automatically after a short period of inactivity
- Maintained with up-to-date operating systems and software
- Used only by the authorised individual when accessing Council systems

6.3 Reasonable care must be taken to ensure that Council data is kept secure at all times.

6.4 Council data must be kept separate from personal data wherever reasonably practicable.

---

7. Email and Communications

7.1 Council business should ordinarily be conducted using official Council email accounts.

7.2 Where personal email accounts are used, users must ensure that:

- Council-related correspondence is copied or forwarded to the Council's official systems
- Records are retained in accordance with Council requirements

7.3 All communications must be professional and appropriate.

7.4 Particular care must be taken when handling personal or sensitive information.

---

8. Access Control and Security

8.1 Access to systems and data shall be granted on the basis of business need.

8.2 Users must:

- Use strong passwords and keep them confidential
- Use Multi-Factor Authentication where available
- Not share accounts or login details

8.3 Access rights shall be reviewed periodically and removed promptly when no longer required.

---

9. Data Management and Protection

9.1 Council data must be stored only within approved systems, such as:

- Council email accounts
- Authorised cloud storage or shared systems

9.2 Council data must not be retained solely on personal devices.

9.3 Data shall be:

- Processed in accordance with data protection principles
- Retained in line with the Council's retention schedule
- Securely deleted when no longer required

9.4 Appropriate arrangements shall be in place to ensure that important records can be recovered if required.

---

10. Working Environment

10.1 Council business is conducted from a variety of locations. Users must ensure that appropriate care is taken to protect Council data and equipment at all times.

10.2 Users must:

- Avoid leaving devices unattended in insecure locations
- Prevent unauthorised viewing or access to information
- Take care when using shared or public networks
- Ensure that confidential discussions cannot be overheard

---

11. Incident Management

11.1 All actual or suspected incidents must be reported to the Clerk without delay. This includes:

- Loss or theft of devices
- Data breaches or suspected breaches
- Unauthorised access to systems or information

11.2 The Council shall maintain a record of incidents and take appropriate action.

11.3 Where required, data breaches shall be reported to the Information Commissioner's Office within statutory timescales.

---

12. Monitoring and Compliance

12.1 The Council reserves the right to monitor the use of its systems, accounts and services to ensure compliance with this policy.

12.2 Any monitoring shall be carried out lawfully, proportionately, and in accordance with data protection legislation.

---

13. End of Role and Access Removal

13.1 When an individual ceases to act on behalf of the Council:

- Access to Council systems shall be removed promptly
- Council data held in personal accounts or on personal devices must be returned or deleted
- The individual may be required to confirm that such data has been deleted

---

14. Breach of Policy

15.1 Failure to comply with this policy may result in appropriate action being taken by the Council, including withdrawal of access to systems or other measures as appropriate.

---

15. Review

15.1 This policy shall be reviewed annually, or sooner if required by changes in legislation or operational requirements.

---

16. Adoption

Adopted by Midgham Parish Council: November 2025
Review: November 2026