Feckenham Parish Council

IT and Data Handling Policy

---

1. Purpose

This policy explains how councillors and the Clerk must use council IT, email and data. It helps the council:

- Work efficiently
- Keep information secure
- Meet legal duties under UK GDPR, FOI and audit requirements
- Protect council equipment and records

Council information is an important asset and must be handled responsibly.

---

2. Who This Applies To

This policy applies to:

- All Parish Councillors
- The Parish Clerk (the only employee)
- Anyone authorised to use council IT systems

---

3. Council IT Equipment

The council owns:

- **One laptop computer (issued to the Clerk)**
- **One printer**

These are recorded in the asset register.

The Clerk is responsible for:

- Safe storage at home
- Keeping equipment secure and updated
- Ensuring it is used only for council work

Equipment must not be shared with family members and must not be left unattended in public places or vehicles overnight.

---

4. Use of Personal Devices (Councillors)

Councillors do **not** receive council laptops or tablets. They use their own devices.

The council is **not responsible** for personal devices.
However, councillors must take **reasonable steps** to protect council information:

- Use a password, PIN, or biometric lock
- Keep the device updated
- Use **two-factor authentication (2FA)** for council email (required)
- Do not share the device with others while council data is open
- Report lost or stolen devices immediately to the Clerk

Council information should not be stored on personal devices longer than necessary.

---

5. Email and Communication

- Only council email accounts must be used for council business
- Personal email accounts must not be used or forwarded to
- Councillors should check email every 1–2 days
- WhatsApp or similar may be used for convenience but not for decisions
- Only the Clerk or Chair may issue official public statements

---

6. IT Security

To protect data:

- Strong passwords must be used and not shared
- Multi-factor authentication (MFA) is used on council email and cloud services
- Devices must lock automatically when not in use
- Antivirus and system updates must be kept current

Council email and cloud storage are provided through **Microsoft 365**, which includes secure hosting, encryption, and backup resilience.

---

7. Data Protection

The council follows UK GDPR principles:

- Only necessary data is collected

- Information is used only for council purposes
- Data is kept secure
- Data is not kept longer than needed

Personal data must not be shared outside the council unless lawful.

The council maintains a **Data Protection Roadmap** to manage ongoing compliance.

---

8. Data Storage and Backups

Council data is stored on:

- The Clerk's council laptop
- Secure Microsoft 365 cloud storage

This system provides backup and recovery if data is lost, damaged or subject to a cyber incident.

Data must not be stored on unencrypted USB devices.

---

9. Data Breaches

If council data is:

- Lost
- Hacked
- Sent to the wrong person
- Accessed without permission

It must be reported to the Clerk **immediately**.

The Clerk will:

1. Record the incident
2. Assess the risk
3. Notify the ICO within 72 hours if required

---

10. FOI and Subject Access Requests

The Clerk is responsible for handling:

- Freedom of Information requests (20 working days)

- Subject Access Requests (1 month)

Councillors must assist if asked to locate information.

---

11. Records and Retention

Emails and documents must be kept according to the Document Retention Policy.

Old or unnecessary data should be deleted regularly.

When a councillor leaves office:

- Access to council systems will be removed
- Council data must be deleted from personal devices

---

12. Audit and Internal Control (AGAR Assertion 10)

This policy supports the council's duty to safeguard assets and records by ensuring:

- Council equipment is protected
- Data is stored securely
- Access is controlled
- Backups exist
- Risks from personal devices are managed

The Clerk is responsible for implementing these controls.

---

13. Monitoring and Compliance

The council may monitor IT and email use to ensure compliance with this policy and the law.

Serious breaches may be reported to auditors or regulators.

---

14. Training

Councillors receive induction on IT and data protection. There is free training available on the Local Government website along with other courses. Should a cost be implemented please do check with the clerk before enrolling. Councillor e-learning | Local Government Association

Alternatively similar courses are available via our County association

https://worcscalc.org.uk/events/elearning/146-essentials-skills/846-data-protection-essentials

There is a rolling programme of courses suitable through Worcs Calc. If you are interested in these do let the clerk know. These sessions are currently available by Zoom and the Council does budget to include them, but you need to check prior to booking.

Training records are kept by the Clerk.

---

15. Review

This policy will be reviewed annually.

Adopted by Feckenham Parish Council on: 10th Feb 2026_____

Signed: _A Smith__ Chair
Signed: __J Bull___ Clerk