GREAT WALDINGFIELD PARISH COUNCIL

GWPC IT Policy v1.0.docx

Contents

1. Purpose

The purpose of this IT Policy is to ensure that Great Waldingfield Parish Council's (GWPC) information technology (IT) systems, data, and digital services are used securely, legally, and effectively. This policy establishes standards for the use, management, and protection of council-owned devices, software, online accounts, and information assets.

2. Scope

This policy applies to:

- All councillors when using council systems or accessing council data.
- The Clerk, RFO, and any other employees or contractors.
- Any volunteer or third party granted access to council information or systems.
- All council-owned devices, cloud services, email accounts, and digital platforms.

3. Legislative and Regulatory Framework

GWPC must comply with the following:

- UK GDPR and the Data Protection Act 2018.
- Freedom of Information Act 2000.
- Local Government Act 1972 (records and governance).
- Public Records Act 1958.
- NCSC Cyber Security Guidance (recommended best practice).
- NALC/SLCC Governance and Accountability for Smaller Authorities.

4. Roles and Responsibilities

4.1 Parish Clerk

- Acts as Data Controller on behalf of GWPC.
- Manages council IT systems, accounts, and data storage.
- Ensures compliance with this policy and relevant legislation.
- Maintains inventories of devices, software, and accounts.

4.2 Councillors

- Use council systems responsibly and in accordance with this policy.
- Protect confidential information.
- Report any suspected data breach or IT incident immediately.

4.3 Contractors / Volunteers

- Must follow this policy when handling council data or systems.
- May only access information authorised by the Clerk.

5. Acceptable Use of IT Systems

5.1 General Principles

- Council IT systems must be used only for council business.
- Personal use of council devices or accounts is prohibited.
- Users must not attempt to bypass security controls.

5.2 Email and Communication

- The official council email address must be used for all council business.
- Councillors should avoid using personal email accounts for council matters.
- Sensitive information must not be sent unencrypted.

5.3 Internet Use

- Users must not access illegal, offensive, or inappropriate content.
- Downloading software or files must be approved by the Clerk.

6. Devices and Equipment

6.1 Council-Owned Devices

- All devices must be password-protected.
- Devices must use up-to-date antivirus and security patches.
- Only authorised users may access council devices.

6.2 Personal Devices (Bring Your Own Device – BYOD)

Where personal devices are used for council business:

- They must have password protection.
- They must not store council data permanently.
- They must use secure email access (e.g., webmail or encrypted apps).
- The Clerk may require remote deletion of council data if necessary.

7. Data Management and Storage

7.1 Data Storage

Council data must be stored:

- In approved cloud services (e.g., Microsoft 365, OneDrive).
- On council-owned devices.
- In accordance with the council's Document Retention Policy.

7.2 Backups

- The Clerk must ensure regular backups of key council documents.
- Backups must be stored securely and separately from primary data.

7.3 Access Control

- Access to data must be granted on a "minimum necessary" basis.
- Passwords must not be shared.
- Multi-factor authentication should be used where available.

8. Cyber Security

8.1 Password Requirements

- Minimum 12 characters.
- Must include a mix of letters, numbers, and symbols.
- Must not be reused across multiple accounts.
- Must be changed immediately if compromised.

8.2 Software Updates

- All devices must install updates promptly.
- Unsupported software must not be used.

8.3 Anti-Malware Protection

- All council devices must run approved antivirus software.
- Users must not disable security tools.

9. Social Media and Website Management

- Only authorised individuals may post on official council platforms.
- Content must be factual, non-political, and compliant with council policies.
- Personal social media accounts must not be used to represent the council.

10. Incident Reporting and Data Breaches

All users must report:

- Loss or theft of devices.
- Suspicious emails or cyber-attacks.
- Accidental disclosure of personal data.

The Clerk must:

- Record incidents.
- Assess whether a breach must be reported to the ICO.
- Implement corrective actions.

11. Procurement and IT Asset Management

- All IT purchases must be approved by the council.
- The Clerk must maintain an asset register including:
    - Devices
    - Software licences
    - Cloud accounts
    - Security credentials

12. Training and Awareness

- Councillors and staff must receive periodic training on:
    - Cyber security
    - Data protection
    - Use of council systems
- New councillors must receive an IT induction.

13. Review and Audit

- This policy must be reviewed annually by the Clerk.
- Significant changes in legislation or technology require earlier review.
- Compliance may be audited as part of internal control checks.

14. Adoption

This IT Policy was adopted by GWPC at its meeting on:

Date: _____

Signed:

Chairman: _____

Clerk: _____

Review Body – GWPC. Reviewed annually and normally each May at the APCM.

15. Version Control

Version	Editor	Date	Comments/Amendments	GWPC Approval
v1.1	MF	13 July 2026	To be accepted by GWPC	GWPC

Appendix 1 – Abbreviations and explanations

APCM - Annual Parish Council Meeting.
Cllr(s) – Councillor(s)
GWPC – Great Waldingfield Parish Council
IT – Information Technology
Mngt – management
Mtg - Meeting
RFO – Responsible Financial Officer
RM – Risk Management
RMS – Risk Management Strategy
SO – Standing Order(s)
PO – Proper Officer
RFO – Responsible Financial Officer