

SIBBERTOFT PARISH COUNCIL

Clerk & RFO: Mrs CE Valentine
c/o 20 Styles Place
Yelvertoft
NN6 6LR
clerk@sibbertoftparishcouncil.gov.uk
www.sibbertoftparishcouncil.gov.uk

Sibbertoft Parish Council – IT Policy

1. Purpose

This policy sets out how Sibbertoft Parish Council manages and uses information technology to ensure legal compliance, data security, accessibility, and good governance. It supports the Council's duty to comply with Assertion 10 of the Annual Governance Statement, which requires councils to have an IT policy and meet digital and data compliance standards.

2. Scope

This policy applies to:

- All councillors
- The Clerk/RFO
- Any volunteers or contractors handling council data
- All devices used for council business (council-owned or personal)

3. Council-Owned Domain & Email Management

To comply with Assertion 10, the Council must operate from a council-owned domain and use official email addresses for all council business.

Requirements

- All official communications must use @sibbertoftparishcouncil.gov.uk email addresses.
- Free email services (e.g., Gmail, Hotmail, Outlook.com) must not be used for council business.
- A generic council email address (e.g., clerk@sibbertoftparishcouncil.gov.uk) must be maintained for continuity.
- Email accounts must be secured with strong passwords and multi-factor authentication where available.

4. Website Management & Accessibility

Assertion 10 requires all councils to meet legal requirements for websites and accessibility.



SIBBERTOFT PARISH COUNCIL

Clerk & RFO: Mrs CE Valentine
c/o 20 Styles Place
Yelvertoft
NN6 6LR
clerk@sibbertoftparishcouncil.gov.uk
www.sibbertoftparishcouncil.gov.uk

Requirements

- The Council website (www.sibbertoftparishcouncil.gov.uk) must comply with:
  - Web Content Accessibility Guidelines (WCAG) 2.2 AA
  - Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
  - Freedom of Information Act 2000 publication scheme requirements
  - Transparency Code for Smaller Authorities (if applicable)
- An Accessibility Statement must be published and reviewed annually.
- All documents uploaded must be accessible (e.g., tagged PDFs, readable text, proper headings).

5. Data Protection & Information Governance

Councils are legally required to comply with GDPR 2016 and the Data Protection Act 2018, acting as both Data Controller and Data Processor.

Requirements

- Personal data must be processed lawfully, fairly, and securely.
- Only the minimum necessary personal data should be collected.
- Data must be stored securely and only retained for as long as necessary.
- Data breaches must be reported to the Clerk immediately for assessment.
- Councillors must use council email accounts for all personal-data-related correspondence to avoid GDPR exposure.

6. Use of Devices (Council-Owned & Personal)

Council-Owned Devices

- Must be used for council business only.
- Must have up-to-date antivirus and security patches.
- Must be password-protected.

Personal Devices

Permitted only if:

- They are password-protected.
- They have up-to-date security software.

- Council data is stored in council-managed systems (e.g., council email, OneDrive).
- Devices are not shared with family members for council work.

7. Cybersecurity

The Council will maintain appropriate cybersecurity measures, including:

- Strong passwords and MFA
- Regular software updates
- Secure cloud storage
- Avoidance of public Wi-Fi for council work unless using a VPN
- Mandatory reporting of suspicious emails or incidents

8. Document Management & Record Keeping

To comply with FOI, GDPR, and the Transparency Code:

- All council documents must be stored in a structured, secure digital filing system.
- Draft documents must be clearly marked.
- Final versions must be retained according to the Council's retention schedule.
- Emails containing decisions or key information must be filed appropriately.

9. Social Media & Digital Communications

- Only authorised individuals may post on behalf of the Council.
- All posts must be factual, neutral, and compliant with the Code of Conduct.
- Personal social media accounts must not be used for official announcements.

10. Training & Awareness

- Councillors and the Clerk must receive periodic training on:
    - Data protection
    - Cybersecurity
    - Accessibility
    - Website management
- Training records will be maintained.



SIBBERTOFT PARISH COUNCIL

Clerk & RFO: Mrs CE Valentine
c/o 20 Styles Place
Yelvertoft
NN6 6LR
clerk@sibbertoftparishcouncil.gov.uk
www.sibbertoftparishcouncil.gov.uk

11. Monitoring & Review

- The Clerk is responsible for monitoring compliance with this policy.
- The policy will be reviewed annually or sooner if legislation changes.
- Non-compliance may be reported in the Annual Internal Audit Report, as required under Assertion 10.

12. Policy Approval

This IT Policy was adopted by Sibbertoft Parish Council on: readopted May 2026

Signed: Chairman: _____ Clerk: _____

Adopted March 2026