



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

1. Introduction

Manston Parish Council, located in Ramsgate, Kent, recognises that robust and carefully governed information technology (IT) systems are critical to the effective delivery of its duties, communications, records management, and public accountability. To this end, this Information Technology Policy (IT Policy) sets out the Council's procedures, standards, and responsibilities in the use of its IT resources—including council-owned computers, mobile devices, networks, software platforms, internet, and email facilities. The policy is designed to comply with all legal, regulatory, and best practice obligations for local government as required in 2025, particularly in light of updated guidance from the Smaller Authorities' Proper Practices Panel (SAPPP), Government Digital Service, the National Cyber Security Centre (NCSC), and relevant data protection law including UK GDPR and the Data Protection Act 2018¹.

This document is a formal policy adopted by Manston Parish Council and applies to all councillors, employees, contractors, and authorised third-parties (including volunteers and temporary staff) who use IT systems for council business, whether on council-owned or personal devices. The policy is structured into clear sections: acceptable use, data protection, cybersecurity, hardware/software management, email and internet usage, business continuity, website management and accessibility, governance, and policy review. It draws from leading practice among UK parish councils and guidance issued in 2025, ensuring that Manston is both compliant and suitably protected against the rapidly evolving landscape of digital risk².

2. Purpose and Scope

The primary objectives of this IT Policy are to:

- Establish clear, practical rules for the use of all IT equipment, email, software, and online systems to ensure efficient, secure, and legal conduct of council business.
- Prevent inappropriate or unlawful use of council IT facilities and data, including personal misuse, copyright violation, loss of data, and exposure to cyber threats.
- Protect the integrity, confidentiality, and availability of council data, including personal and commercially sensitive information, as required under UK GDPR.
- Ensure effective management of council hardware and software assets, and secure use of personal devices for council work (BYOD).
- Promote transparency, accountability, and accessibility in council operations, particularly regarding website management and the publication of council documents³⁴.

The scope of this policy covers:

- All IT systems and resources owned, leased, or managed by Manston Parish Council.
- The Council's official emails, online storage, and websites.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

- Use of personal devices to access or process council information (BYOD).
 - All persons who handle council data, including councillors, officers, contractors, and volunteers⁵.
-

3. Governance, Roles, and Responsibilities

3.1 Council and Clerk Responsibilities

The overall accountability for IT governance, compliance, and security rests with the Parish Council. Day-to-day administration of IT resources and data protection compliance is delegated to the Parish Clerk—currently clerk@manstonparishcouncil.gov.uk⁶.

The Clerk's core IT responsibilities include:

- Maintaining an up-to-date asset register for council-owned hardware and software.
- Acting as the council's Data Protection Compliance Officer and the point of contact for all IT-related incidents or queries.
- Managing access to council data and systems, including setting up, modifying, and closing email/user accounts as roles change.
- Ensuring training and awareness on IT policy provisions for all councillors and staff.
- Overseeing the implementation, monitoring, and annual review of this IT Policy.

Council staff and councillors are responsible for reading, understanding, and adhering to this policy at all times. Non-compliance will be subject to disciplinary or remedial procedures³⁷⁴.

3.2 Delegation and Escalation

Where practical, certain IT management tasks (such as procurement, technical support, or cybersecurity risk assessment) may be delegated to qualified contractors or service providers, under appropriate contractual controls. Any suspected breach of policy, security incident, or data protection concern must be reported immediately to the Clerk, who will escalate as necessary to the Council Chairman or external bodies (such as the ICO), according to the documented incident response plan⁸⁹.

4. Acceptable Use Policy

4.1 General Principles

Council IT resources (including computers, mobile devices, storage, networks, email accounts, and cloud services) must be used solely for authorised council business or functions. Usage by councillors, staff, or authorised third parties for private purposes is permitted only to a minimal and



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

incidental extent, provided it does not interfere with council operations, security, or contravene this or any related policy¹⁰.

Usage is expressly prohibited for:

- Illegal or unlawful activities of any kind.
- Personal, political, commercial, or income-generating activity.
- Accessing, storing, or transmitting offensive, abusive, defamatory, racist, sexist, or harassing material.
- Sharing confidential council or personal data with unauthorised parties.
- Downloading, copying, or installing unlicensed or unauthorised software or multimedia content.
- Circumventing or attempting to disable IT security controls.

All users shall exercise caution, respect copyright and intellectual property rights, and avoid the use of council IT resources in any manner that could cause reputational harm to the council, its partners, or residents³¹¹.

4.2 Device and Network Usage

- Only council-issued hardware and authorised devices may be used to access confidential council systems. The use of private devices is governed by the BYOD policy in this document.
- Unauthorised installation of software (including freeware and apps) on council devices is strictly prohibited. Applications must be approved and installed by, or under the supervision of, the Clerk.
- Users must not attempt to connect hardware, peripherals, or media (e.g., USB drives) to council computers without prior consent.
- All use of the Internet and council network must be professional, relevant to council duties, and conducted with care to avoid exposure to online threats (see Cybersecurity).
- Personal use of internet access should be minimal, outside core working time, and must not include the downloading of software or accessing inappropriate material³¹¹.

4.3 Monitoring and Audit

The Council reserves the right to monitor, inspect, and audit any use of its IT facilities—including email, internet usage, and device logs—within legal parameters and where required to ensure compliance, investigate breaches, or support legal proceedings. This may include outsourced or third-party audits as appropriate, but must respect individual data privacy rights except where overridden by statutory requirements¹⁰³.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

5. Data Protection and GDPR Compliance

5.1 Data Controller Responsibilities

Manston Parish Council is both Data Controller and Data Processor for information it holds on residents, staff, elected officials, contractors, and service users. This includes all personal data (as defined by UK GDPR), including names, contact details, correspondence, application forms, and minutes. Special category and sensitive personal data must be treated with additional care and legal safeguards¹²¹³.

5.2 Data Protection Principles

Council personnel and contractors must ensure that personal data is:

- Processed fairly, lawfully, and transparently.
- Collected only for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary for those purposes.
- Accurate and (where applicable) kept up to date.
- Kept for no longer than is necessary and securely destroyed when retention ends.
- Protected by appropriate technical and organisational measures against unlawful access, loss, damage, or destruction¹²¹⁴.

Details of data storage, access control, backup, retention and destruction must adhere to the council's Data Protection Policy, which is read alongside this IT Policy.

5.3 Data Breach, Subject Access, and Rights

Any suspected or actual data breach—including loss of a device, unauthorised access, or accidental disclosure—must be reported immediately to the Clerk. The breach will be assessed, contained, and, if necessary, reported to the ICO within 72 hours as per statutory guidelines⁸⁹¹².

Data subjects have rights of access, rectification, erasure, restriction, portability, and objection to processing. Requests must be acknowledged and responded to in line with statutory timescales, utilising secure communications and identity checks¹³.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

6. Cybersecurity Policy

6.1 Core Cybersecurity Principles

Manston Parish Council adopts a layered cybersecurity approach, following the NCSC's 10 Steps to Cyber Security Framework and the latest Government guidance for public sector entities. The main principles include:

- Maintaining up-to-date asset and risk registers for all critical IT, data, and supplier dependencies.
- Enforcing strong authentication for all users (including complex passwords, two-factor authentication where available).
- Restricting system access to the principle of least privilege and promptly removing access for leavers.
- Preventing, detecting, and responding to malware, phishing, and cyber-attacks using up-to-date antivirus software and threat monitoring.
- Ensuring systematic, verifiable data backup, recovery, and business continuity planning.
- Embedding cybersecurity awareness among all staff/councillors through periodic training, phishing simulation, and policy refreshers ¹⁵¹⁶¹⁷.

6.2 Incident Response Plan

The Clerk is responsible for the Council's incident response coordination. The Council will maintain an incident response plan (IRP) specifying:

Incident Type	Action Steps	Escalation
Suspected Breach	Isolate affected systems, preserve evidence, inform Clerk	Escalate to Chair, assess regulatory notification
Lost Device	Attempt remote lock/wipe, change passwords, report to Clerk & police	Notify data subjects/ICO if personal data at risk
Phishing Attack	Warn users, investigate scope, reset credentials, run malware scan	Review controls, re-train staff as necessary
Ransomware Attack	Invoke business continuity, seek external IT support, preserve logs	Brief council, liaise with insurers, inform ICO if data affected

All incidents must be logged and reviewed post-event to update procedures and train personnel accordingly.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

Business/student continuity plans must be tested annually and include cyberattack scenarios.⁸

6.3 Cyber Insurance

The Council will review and hold cyber insurance coverage appropriate to its risk profile, ensuring prompt access to technical and legal support in the event of a significant incident¹⁶.

7. Hardware and Software Asset Management

7.1 Asset Inventory and Registration

All council-owned IT hardware (laptops, desktops, tablets, mobile devices, printers, storage media) must be entered into an asset register maintained by the Clerk. The register records:

- Device model, unique asset ID, serial number.
- Date/location of purchase/issuance.
- Owner or user assignment.
- Warranties/support status, maintenance records.
- Current software and licensing state.

Regular audits will verify the location, condition, and use of all registered assets¹⁸¹⁹²⁰.

7.2 Device Protection and Controls

- All devices must be protected through appropriate physical and electronic security:
 - Password-protected screensavers with short auto-lock intervals.
 - Encryption enabled (particularly for portable devices).
 - Device locks/cable attachments for public/communal settings.
- Lost, stolen, or end-of-life devices must be reported immediately, with the Clerk ensuring that any data-bearing device is securely wiped or physically destroyed, with written evidence retained for audit purposes.
- Only authorised staff may install, configure, or move council hardware.

7.3 Software Licensing and Security

- Only council-authorised and appropriately licensed software can be used on council devices.
- Copies, downloads, or installations of unlicensed or unauthorised software are strictly prohibited and a criminal offence under the Copyright, Designs and Patents Act 1988.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

- Software patching and updates (including urgent security patches) shall be scheduled and centrally managed.
- All software in active use must be supplier-supported and reviewed periodically for obsolescence or vulnerabilities.
- Where business applications are replaced or retired, all associated software and data must be archived, migrated, or securely deleted through verifiable procedures¹⁹²⁰.

8. Bring Your Own Device (BYOD) Policy

8.1 Scope and Use

Where permitted and with explicit authorisation from the Clerk, councillors or staff may use their own personal laptops, mobile phones, or tablets (BYOD) for council business. This practice recognises practical realities for small councils but carries intrinsic risks that must be managed via the following rules³²¹²²⁵.

8.2 Minimum Requirements

Personal devices used for council business must:

- Be protected with a secure password/PIN/biometric authentication.
- Have up-to-date operating system security patches and antivirus software.
- Use device encryption, particularly for any storage of council data.
- Not be used to download, store, or transmit council data using non-approved applications or cloud storage.
- Ensure prompt deletion of council data/emails when no longer required, or on termination of office.
- Not be backed up to personal or third-party cloud accounts not approved by the council.
- Prohibit removable, unencrypted storage of council data (no council data on USB sticks or SD cards except with explicit approval and secure encryption).

Loss, theft, or suspected compromise of a BYOD device containing council data must be reported to the Clerk immediately, to enable rapid risk assessment, any remote wipe, and regulatory notification where necessary³²¹²²⁵.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

9. Email and Internet Usage Policies

9.1 Council Email Protocol

- All official council communications must be conducted through a council-provided and council-owned email address (e.g., clerk@manstonparishcouncil.gov.uk).
- Generic, permanent role-based email accounts may be established (e.g., clerk@...; chairman@...; info@...), not personal accounts (e.g., joebloggs@gmail.com). Private email accounts **must not** be used for council business under any circumstances from 2025, as explicitly required under SAPP Assertion 10¹²³.
- Email forwarding to personal or other non-council addresses is strictly prohibited.
- Email accounts and data must be strictly controlled when councillors/staff leave office, with prompt revocation of access and secure deletion of all council data from personal devices.

9.2 Security and Conduct

- All users must exercise caution with emails, particularly those containing attachments, links, or unexpected content—even if apparently sent from a known source. Phishing and malware are major risks and must be reported immediately if suspected¹⁰.
- Confidential or personal information may only be sent by email as an encrypted attachment or secure link. Passwords must be sent separately from the content.
- Use professional language in all email correspondence. Do not transmit, create, or forward material that could bring the Council into disrepute or infringe copyright, defamation, privacy, or discrimination laws.
- Council email will be monitored for compliance and to support security investigations, with due respect for data privacy except as overridden by law, audit, or incident response needs.

9.3 Internet Usage

- Internet access is provided to support council functions. Personal use may be permitted if minimal, not at the expense of council business, and never for accessing, downloading, or sharing inappropriate or illegal content.
- Downloading any software or files from the internet (outside official platforms) to council devices is strictly prohibited unless verified by the Clerk. All downloads must be scanned for viruses/malware before use.
- Social media and online forum activity on behalf of the Council is restricted to official accounts managed by the Clerk or as delegated, with clear distinction between personal views and official council communications³.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

10. Website Management and Accessibility

10.1 Website Operation

The Council's website (www.manstonparishcouncil.gov.uk) is a central means of communication, public transparency, and document sharing. The Clerk (or a nominated web officer) is responsible for publishing updates, maintaining records, and monitoring security and accessibility compliance²⁴²⁵.

All required documents—including meeting agendas and minutes, statutory notices, annual returns, declarations of members' interests, and transparency code data—must be published promptly and archived for required periods.

10.2 Accessibility

From October 2024, the Council website and all published online materials must conform to Web Content Accessibility Guidelines (WCAG) 2.2 AA standards, as mandated by the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 (as amended). This ensures all users, including those with disabilities, can access information and services with equal effectiveness²⁵²⁶²⁷.

The website must, where practicable:

- Be compatible with screen readers, assistive technologies, and diverse browsers/devices.
- Carry an up-to-date Accessibility Statement detailing the council's compliance position, accommodations for non-accessible content, and channels for requesting alternative formats.
- Undergo regular audits to validate accessibility and correct identified issues.

10.3 Website Security and Data

- The website must employ SSL encryption and ensure secure management of administrator accounts, with strong, unique passwords and two-factor (or multi-factor) authentication.
- Admin access must be removed for departing staff/councillors promptly.
- No unnecessary retention of user data: contact forms and submission data must be purged regularly and processed only for their legitimate purpose¹⁷²⁵.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

11. Training and Awareness

11.1 General Training

All councillors, staff, and authorised users of council IT facilities must complete induction training covering:

- Acceptable use of IT resources.
- Cybersecurity essentials, including phishing and social engineering threats.
- Data protection/GDPR responsibilities and privacy procedures.
- Secure password and device management.
- Website and accessibility obligations.
- How to report IT security incidents and data breaches¹⁵³.

Training must be updated at least annually, and after any significant policy change or major IT incident. Periodic awareness campaigns (e.g., simulated phishing exercises) are strongly encouraged.

11.2 Policy Review and Maintenance

This policy shall be reviewed at least annually by the Clerk (or nominated IT officer), with any changes approved by full Council and formally minuted. Reviews shall take into account:

- Technology and threat landscape changes.
- Changes to data protection, accessibility, or digital compliance law (including any updates to SAPP Guidance, Government Digital Service standards, NCSC frameworks).
- Practical feedback from users and audit/incident reports.
- Amendments to council operations or service providers.

Adoption, version control, and the minutes of approval and review dates must be maintained for audit purposes²²⁸³.

12. Policy Breach, Enforcement, and Sanctions

Policy breaches—whether intentional, reckless or through negligence—may result in withdrawal of IT privileges, disciplinary action (up to and including removal from office or dismissal), and, where relevant, referral to law enforcement, the Information Commissioner’s Office, or external auditors. Users have a duty to report actual or suspected breaches promptly to the Clerk.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

Mechanisms must be in place to investigate alleged breaches, take appropriate sanctions, and pursue lessons-learned for procedural improvements and future risk mitigation³⁷¹⁰.

13. Policy Table: Summary of Core Areas and Controls

Policy Area	Key Controls and Expectations	Responsible Party	Review Frequency
Acceptable Use	Council business only; no personal gain/illegal use; professional conduct	All users	Annual
Data Protection & GDPR	Lawful, fair, minimal, secure processing; prompt breach reporting	Clerk/Data Officer, all users	Annual/re: GDPR
Cybersecurity	Password hygiene; antivirus; backups; incident response; risk review	Clerk (with external support if needed)	Annual/After event
Asset Management	Asset register; secure handling; approved purchasing/disposal	Clerk	Annual
Software Licensing	Only licensed/approved software; central installation; patch management	Clerk/approved IT provider	Annual
BYOD	Secure BYOD permitted; encryption; no unauthorised access	All users; Clerk oversight	Annual
Email & Internet Use	Role-based council accounts only; monitoring; professional language	All users	Annual
Website & Accessibility	WCAG 2.2AA standard; Accessibility Statement; SSL; admin access control	Clerk/Web Editor	Annual/Quarterly
Training & Policy Review	Induction and annual refresher training; formal review/minutes	Clerk/Training Officer	Annual
Enforcement	Investigation and sanctions for breach; lessons-learned for the future	Clerk; Full Council	As necessary



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

14. Legal and Statutory Compliance

This policy is drafted to comply fully with:

- The Local Government Act 2000 and subsequent relevant local government legislation.
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018¹²¹³¹⁴.
- Freedom of Information Act 2000 and Transparency Code for Smaller Authorities.
- SAPP 2025 Practitioners' Guide, including Assertion 10: Digital and Data Compliance²⁹²¹.
- The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and WCAG 2.2 AA Standard²⁷²⁵.
- NCSC and Government Digital Service technology, cybersecurity and incident management guidance.

Updates to this document will reference changes to the above standards and best practice recommendations by sector bodies such as NALC and SLCC⁴.

15. Additional Provisions & Appendices

15.1 Appendix—Data Breach Response Checklist

- Contain: Remove device from network, secure premises/data, preserve evidence.
- Assess: Risk to data subjects, type and quantity of data involved.
- Notify: Inform Clerk, assess ICO and data subject notification requirements.
- Remediate: Change credentials, deploy technical fixes, review incident.
- Review: Update relevant policy/practice, provide feedback/training to users involved.

15.2 Appendix—Change Control & Joiners/Leavers Process

- New user: Training, provision of secure IT, allocation of email and system accounts.
- Leaver: Recovery of all devices, immediate revocation of accounts, secure deletion of held council data on BYOD.



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

16. Adoption, Review Cycle, and Public Availability

- **Adopted by Manston Parish Council:** 10 November 2025
- **Review Date:** 10 November 2026
- **Responsible:** Parish Clerk, with oversight by Council Chairman
- **Contact Address:** Manston Parish Council, www.manstonparishcouncil.gov.uk
|clerk@manstonparishcouncil.gov.uk

This policy shall be published on the council website for public review, with full compliance statements and linked accessibility and data protection policies as appropriate.

17. Closing Statement

The adoption, implementation, and regular review of this Information Technology Policy are both a statutory and operational necessity for Manston Parish Council in 2025 and beyond. Compliance with SAPP's digital and data standards, the statutory data protection, transparency, and accessibility obligations, and ongoing vigilance in the face of cyber threats are critical to upholding public trust, legal obligations, and operational resilience.

All users of council IT resources must read and adhere to this Policy. A digital copy is available from the council website, and copies are issued as part of the induction of any new staff member, councillor, or contractor.

End of Document

References (29)

- 1 *Assertion 10 (SAPP 2025) - Council IT Policy | Aubergine.* <https://www.aubergine262.com/assertion-10-2025-practitioners-guide-it-policy/>
- 2 *Parish Council Governance Update and Policy Implementation Plan.* https://www.girton-cams.org.uk/wp-content/uploads/2025/07/Parish_Council_AGAR2025_Policy_Guide.pdf
- 3 *IT Policy I - Pembury Parish Council.* <https://pemburyparishcouncil.gov.uk/wp-content/uploads/2023/05/230515-IT-Policy-ADOPTED.pdf>
- 4 *Information Technology Policy Guidelines.* <https://www.nalc.gov.uk/resource/information-technology-policy-guidelines.html>



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

5 *Bring Your Own Device (BYOD) Policy – Corfe Castle Parish Council.*

<https://www.corfecastleparishcouncil.gov.uk/bring-your-own-device-byod-policy/>

6 *Manston Parish Council | Parish Councils.* <https://www.parishcouncils.uk/parish-council/manston-parish-council-2/>

7 *ST LEONARDS & ST IVES PARISH COUNCIL.* <https://stleonardsparishcouncil.gov.uk/wp-content/uploads/2025/08/20.-IT-and-Cyber-Security-Policy.pdf>

8 *Capel St Mary Parish Council.* <https://capelstmary.onesuffolk.net/assets/Parish-Council-Documentation/2024/GDPR/Cyber-security-checklist-and-security-incident-policy-February-2024.pdf>

9 *Security Incident Response Policy.* <https://www.whittingtonparishcouncil.gov.uk/wp-content/uploads/sites/117/2025/06/WhitPC-Security-Incident-Response-Policy-2025-26.pdf>

10 *Acceptable use policy - Enfield Council.* <https://www.enfield.gov.uk/services/your-council/our-policies-and-procedures/acceptable-use-policy>

11 *BRANDON & BYSHOTTLES PARISH COUNCIL.*

<https://brandonandbyshottlesparishcouncil.gov.uk/wp-content/uploads/2025/06/23.1-Acceptable-Use-of-Computer-Email-Facilities-Policy.pdf>

12 *DATA PROTECTION POLICY (UK GDPR COMPLIANT).*

<https://www.tatenhillrangemoreparishcouncil.gov.uk/wp-content/uploads/sites/135/2025/09/Data-protection.pdf>

13 *Information and General Data Protection Policy.*

<https://www.dbhparishcouncil.uk/media/attachments/2025/05/29/information-and-general-data-protection-policy-2025.pdf>

14 *Data Protection Policy (UK GDPR Compliance) – Wedmore Parish Council.* <https://wedmore-pc.gov.uk/documents/data-protection-policy-uk-gdpr-compliance/>

15 *Exploring the NCSC's 10 Steps to Cyber Security - Intrasource.*

<https://www.intrasource.co.uk/blog/it-security/exploring-the-ncscs-10-steps-to-cyber-security/>

16 *Strengthening Cyber resilience in Parish and Local Councils in 2025.*

<https://www.clearcouncils.co.uk/uncategorised/strengthening-cyber-resilience/>

17 *Is your council ready for the Cyber Assessment Framework?.* <https://www.aubergine262.com/is-your-council-ready-for-the-cyber-assessment-framework/>

18 *Principle: A3 Asset Management - UK Government Security - Beta.*

<https://www.security.gov.uk/policy-and-guidance/government-cyber-security-policy-handbook/principle-a3-asset-management/>



Information Technology Policy for Manston Parish Council

Adopted: 10 November 2025 — Next Review date: 10 November 2026

19 *Hardware Asset Management Policy - Capita.*

<https://www.capita.co.uk/sites/g/files/nginej291/files/2024-07/Hardware-Asset-Management-Policy-v4.0.pdf>

20 *Asset management | ICO.* <https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/information-and-cyber-security/asset-management/>

21 *HELSEBY PARISH COUNCIL.* <https://www.helsbyparishcouncil.gov.uk/wp-content/uploads/sites/116/2025/07/Bring-Your-Own-Device-Policy-25.pdf>

22 *Bring Your Own Device (BYOD) Policy -September 2023.*

<https://buckleshamparishcouncil.gov.uk/assets/Parish-Council/Parish-Council-Documents/BPC-Bring-Your-Own-Device-Policy-202309.pdf>

23 *A 5-Minute Masterclass In Web Accessibility.* https://hiltonparishcouncil.com/wp-content/uploads/2025/05/25-26-90.-CAPALC_Assertion-10-webinar-2025.pdf

24 *Manston Parish Council, Manston, Ramsgate.*

<https://www.manstonparishcouncil.gov.uk/community/manston-parish-council-15572/home/>

25 *Gov Domains plus a WCAG 2.2 & GDPR Compliant Parish Website.*

<https://myparishcouncil.co.uk/gov-domain-GDPR-wcag-compliant>

26 *Parish Council Websites | Town Council Websites - Aubergine.*

<https://www.aubergine262.com/parish-town-council-websites/>

27 *WCAG2.2AA Compliant Accessible Websites - SLCC.* <https://www.slcc.co.uk/wcag-website-compliance-for-councils/>

28 *Draft Policy Review Schedule April 2018.* <https://melbournparishcouncil.gov.uk/wp-content/uploads/2025/05/PC014-2526e-Document-0.00-Policy-Review-Schedule-May-2025-DRAFT.pdf>

29 *SAPPP 2025 - Why Every Parish and Town Council Now Needs an IT Policy.*

<https://www.scribeaccounts.com/blog/sapp-2025---why-every-parish-and-town-council-now-needs-an-it-policy>