Great Bromley Parish Council
Information Technology, Digital Governance & Data Risk Management Policy

1. Purpose
This policy sets out how the Parish Council manages and protects its information technology, digital systems, and data. It ensures compliance with UK legislation and with AGAR Assertion 10, which requires councils to maintain secure, accessible, and well-governed digital arrangements. It also incorporates the Council's Overall Digital & Data Risk Assessment, reviewed annually.

2. Scope
This policy applies to:
- All councillors, employees, contractors, and volunteers acting on behalf of the Council
- All council-owned IT equipment (laptops, desktops, tablets, smartphones)
- All software, cloud services, email systems, and online platforms used for council business
- Any personal devices used for council work under approved Bring-Your-Own-Device (BYOD) arrangements

3. Digital Governance Requirements (AGAR Assertion 10)
To meet Assertion 10, the Council will:
- Operate a council-owned domain name for its website and email services
- Provide and require the use of official council email accounts for all council business
- Maintain a generic council email address (e.g., clerk@parishcouncil.gov.uk)
- Maintain a website that meets WCAG 2.2 AA accessibility standards
- Publish information required by the Transparency Code and FOI Publication Scheme
- Maintain an Overall Digital & Data Risk Assessment, included within this policy
- Ensure all digital systems are secure, backed up, and appropriately managed

4. Acceptable Use
- Council IT equipment and services must be used primarily for council business.
- Limited personal use is permitted if it does not interfere with duties or breach policy.
- Users must not access, store, or transmit illegal, offensive, or discriminatory material.
- All use must comply with UK law, including copyright and licensing rules.

5. Passwords and Access Control
- Strong, unique passwords must be used for all council systems.
- Passwords must not be shared or stored insecurely.
- Access to systems and data will be granted only where necessary for the role.
- Multi-factor authentication (MFA) must be enabled where available.

6. Data Protection and Confidentiality
- All users must comply with UK GDPR and the Data Protection Act 2018.
- Personal data must be stored securely and accessed only by authorised individuals.
- Confidential information must not be disclosed without proper authority.
- Any suspected data breach must be reported immediately to the Clerk.

7. Email and Communication
- All council business must be conducted using official council email accounts.
- Personal email accounts must not be used for council work.
- Email must be written professionally and handled with care, especially when dealing with sensitive information.
- Emails must be retained, archived, or deleted in line with the Records Management Policy.
- When a councillor leaves office, their council email account must be closed and archived.

8. Internet and Online Services

- Internet access must be used responsibly and primarily for council business.
- Downloading unauthorised or pirated software is prohibited.
- Users must not access or distribute inappropriate content.
- Cloud services must be approved by the Council before use.

9. Software, Security and Updates

- Only approved software may be installed on council devices.
- All devices must have up-to-date antivirus protection and security patches.
- Users must not disable or alter security settings without authorisation.
- Devices must lock automatically after a short period of inactivity.

10. Use of Personal Devices (BYOD)

Personal devices used for council business must:

- Have password or biometric protection
- Use encryption where available
- Have up-to-date security software
- Store council data separately from personal data
- Allow council data to be deleted remotely if required

Council data must be removed from personal devices when no longer needed or when the user leaves the Council.

11. Website Management and Accessibility

- The Council must maintain a website that complies with WCAG 2.2 AA accessibility standards.
- An up-to-date Accessibility Statement must be published.
- Required documents must be published in accessible formats.
- The website must be securely hosted and backed up regularly.

12. Transparency and Publication Duties

The Council must publish information required by:

- The Transparency Code for Smaller Authorities
- The Freedom of Information Act Publication Scheme
- The Local Government Act 1972 (agendas, minutes, notices)
- The Accounts and Audit Regulations (AGAR documents)

13. Equipment Management

- All council-owned IT equipment remains the property of the Parish Council.
- Equipment must be returned upon leaving the Council or on request.
- Loss, theft, or damage must be reported immediately.

14. Backups and Records Management

- Important council data must be backed up regularly to secure, approved locations.
- Electronic records must be managed in line with the Council's Records Management Policy.
- Backups must be tested periodically to ensure they can be restored.

Overall Digital & Data Risk Assessment
(Integrated into this policy for AGAR Assertion 10 compliance)

15. Risk Assessment Summary
A. Governance & Compliance Risks

Risk	Impact	Likelihood	Controls in Place	Residual Risk
Non-compliance with AGAR Assertion 10	Audit failure; reputational damage	Low	Policy adopted; annual review; domain-based email; accessibility compliance	Low
Failure to meet Transparency Code or FOI duties	Legal non-compliance; complaints	Medium	Publication schedule; Clerk oversight; accessibility statement	Low
Inadequate data protection practices	ICO enforcement; data breach	Medium	GDPR training; secure storage; access controls; breach procedure	Low

B. Email, Communication & Identity Risks

Risk	Impact	Likelihood	Controls in Place	Residual Risk
Use of personal email for council business	Loss of records; GDPR breach	Medium	Mandatory council-domain email; retention rules	Low
Loss of access when councillors leave	Missing records; FOI issues	Medium	Centrally managed accounts; closure & archive process	Low
Phishing or malicious emails	Malware; data loss	Medium	User awareness; antivirus; MFA	Medium–Low

C. Device & Equipment Risks

Risk	Impact	Likelihood	Controls in Place	Residual Risk
Loss or theft of council device	Data breach	Low	Encryption; passwords; remote wipe	Low
Out-of-date software	Vulnerability to attack	Medium	Automatic updates; annual audit	Low
Unauthorised software installation	Malware; licensing issues	Low	Approved-software list	Low

D. Website & Online Publishing Risks

Risk	Impact	Likelihood	Controls in Place	Residual Risk
Website not meeting WCAG 2.2 AA	Legal non-compliance	Medium	Accessibility statement; accessible templates	Low
Website outage or hosting failure	Loss of public information	Low	Reputable hosting; backups	Low
Incorrect or missing published documents	Audit queries	Medium	Clerk publication checklist	Low

E. Data Storage, Backup & Records Risks

Risk	Impact	Likelihood	Controls in Place	Residual Risk
Loss of council data	Operational disruption	Low	Cloud storage; backups	Low
Poor retention or deletion	FOI/GDPR non-compliance	Medium	Records Management Policy	Low
Unauthorised access	Data breach	Low	Access controls; MFA; encryption	Low

F. Personal Devices (BYOD) Risks

Risk	Impact	Likelihood	Controls in Place	Residual Risk
Council data stored insecurely	GDPR breach	Medium	BYOD rules; encryption	Medium–Low
Loss of personal device containing council data	Data breach	Medium	Password protection; reporting procedure	Medium–Low

16. Risk Control Measures

- Technical controls: MFA, encryption, antivirus, secure cloud storage, automatic updates
- Administrative controls: this policy, Records Management Policy, councillor onboarding, accessibility compliance
- Physical controls: secure storage of devices, reporting of loss/theft, return of equipment

17. Monitoring and Review

- The Clerk reviews digital and data risks annually and reports to the Council.
- Additional reviews take place following a data breach, legislative change, or major IT change.
- This combined policy and risk assessment is published on the Council website.

18. Adoption

This policy and risk assessment were adopted by Great Bromley Parish Council at its meeting on Wednesday 11 March 2026 and will be reviewed annually.