



Parish Clerk
King George V Playing Fields Pavilion
Front Street, Framwellgate Moor, Durham, DH1 5BL

07572 004256
clerk@framwellgatemoorparish.gov.uk

INFORMATION TECHNOLOGY (IT), EMAIL AND DATA SECURITY

POLICYFRAMWELLGATE MOOR PARISH COUNCIL

Details

Policy	Adopted	Author
Information Technology (IT), Email and Data Security	June 2026	Craig Eddon

Version

Date	Ref	History	Revised by
27/05/26	V1		Craig Eddon

Review

Review	Last Review	Next Review	Principal Reviewer
Annually	May 2026	March 2027	Clerk

Framwellgate Moor Parish Council (“the Council”) recognises the importance of effective and secure information technology (IT), email and data management in supporting the Council’s business, operations, governance and communications.

This policy outlines the standards, responsibilities and expectations relating to the use of IT systems, electronic communications and data handling by councillors, employees, contractors and volunteers acting on behalf of the Council.

The Council is committed to ensuring compliance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- Freedom of Information legislation
- The Accounts and Audit Regulations 2015
- The Transparency Code for Smaller Authorities
- Relevant cyber security and accessibility guidance

Scope

This policy applies to:

- councillors;
- employees;
- volunteers;
- contractors;
- and any individual using Council IT systems, email accounts, devices or data.

The policy applies to:

- Council-owned devices;
- personal devices used for Council business;
- Council email accounts;
- cloud storage systems;
- Council website administration;
- and all electronically stored Council information.

Council IT Arrangements

The Council uses digital systems to support communication, financial administration, document storage and governance functions.

The Council currently operates:

- official Council email accounts using the Council’s domain;
- cloud-based storage and backup arrangements provided through Net Power Creative using iCloud storage arrangements;
- website and electronic publication systems;
- internet banking and accounting software;
- and electronic agenda and minute distribution systems.

The Clerk/RFO is responsible for overseeing the day-to-day administration of the Council’s IT arrangements.

Acceptable Use of IT Resources

All users of Council IT resources must:

- use systems responsibly and lawfully;
- protect confidential and sensitive information;
- maintain professional standards in electronic communications;
- avoid accessing, storing or distributing inappropriate, offensive or illegal material;
- and comply with this policy and associated Council procedures.

Council IT resources must primarily be used for official Council business.

Users must not:

- install unauthorised software;
- share passwords;
- bypass security controls;
- or use Council systems in a manner likely to damage the Council's reputation or breach legal obligations.

Use of Personal Devices

The Council recognises that councillors and staff may occasionally use personal devices for Council business.

Where personal devices are used, users must ensure:

- devices are password protected;
- software and operating systems are regularly updated;
- anti-virus and security protections are maintained where appropriate;
- confidential information is stored securely;
- and Council information is deleted securely when no longer required.

Reasonable steps must be taken to separate Council information from personal information where possible.

Passwords and Account Security

All users are responsible for maintaining the security of Council accounts and passwords. Passwords should:

- be strong and unique;
- not be shared;
- and be changed if compromise is suspected.

Users are encouraged to use password managers and multi-factor authentication where available.

Login details required for business continuity purposes should be securely retained so authorised persons can access Council systems if required.

Email Communications

The Council will endeavour to provide official Council email accounts for Council-related communications.

Councillors and staff are encouraged to use official Council email accounts for Council business in accordance with current government and sector guidance.

Emails sent on behalf of the Council must:

- be professional and respectful;
- comply with data protection requirements;
- avoid disclosing confidential information inappropriately;
- and not contain offensive, abusive or defamatory content.

Care should be taken when opening attachments or clicking links to avoid phishing attacks, malware and fraudulent activity.

Any suspicious emails or cyber security concerns should be reported immediately to the Clerk/RFO.

Email Management and Correspondence

Routine correspondence received by the Council may be dealt with by the Clerk under delegated powers where appropriate.

Correspondence requiring Council consideration may:

- be placed on a Council agenda;
- be circulated to councillors;
- or be acknowledged pending Council consideration.

The Council reserves the right not to respond to vexatious, abusive or unreasonable correspondence in accordance with relevant legislation and Council procedures.

All Council correspondence remains subject to:

- Freedom of Information legislation;
- Subject Access Requests;
- and legal disclosure requirements.

Data Protection and Information Security

All personal and confidential information must be:

- processed lawfully, fairly and transparently;
- stored securely;
- protected against unauthorised access, loss or disclosure;
- and retained only for as long as necessary.

Users handling personal information must comply with:

- UK GDPR;
- the Data Protection Act 2018;
- and Council privacy and retention policies.

Electronic records containing sensitive information should only be shared where necessary and through secure methods.

Data Storage, Retention and Backup

The Council maintains electronic records and backups through cloud-based storage arrangements.

The Council uses iCloud-based storage arrangements provided through Net Power Creative to support secure off-site backup and continuity of records.

Important Council records should be retained in accordance with the Council's retention arrangements and legal obligations.

The Clerk/RFO is responsible for ensuring important records are appropriately backed up and recoverable where reasonably practicable.

Website, Accessibility and Transparency

The Council will maintain a website that seeks to comply with:

- website accessibility legislation;
- the Transparency Code for Smaller Authorities;
- and publication requirements under relevant legislation.

The Council will publish statutory information including:

- agendas and minutes;
- AGAR and audit documents;
- policies and governance documents;
- and public notices where required.

Cyber Security and Incident Reporting

All users must remain vigilant against cyber threats including:

- phishing emails;
- malware;
- fraudulent payment requests;
- and unauthorised access attempts.

Any suspected:

- data breach;
- cyber incident;
- loss of device;
- or security concern

must be reported immediately to the Clerk/RFO.

The Council will investigate incidents appropriately and take action where required.

Monitoring and Compliance

The Council reserves the right to monitor use of Council IT systems and email accounts where necessary to:

- ensure compliance with this policy;
- investigate potential breaches;
- protect Council data;
- and comply with legal obligations.

Monitoring will be proportionate and undertaken in accordance with data protection legislation.

Failure to comply with this policy may result in:

- withdrawal of access to Council systems;
- referral under relevant Council procedures;
- or legal action where appropriate.

14. Training and Awareness

The Council recognises the importance of ongoing awareness and good practice in IT and cyber security.

Councillors and staff are encouraged to:

- undertake relevant cyber security awareness training;
- remain alert to scams and phishing attempts;
- and follow current guidance issued by recognised bodies including:
 - the National Cyber Security Centre (NCSC);
 - CDALC;
 - and the Smaller Authorities Proper Practices Panel (SAPP).

Policy Review

This policy will be reviewed annually by Framwellgate Moor Parish Council or sooner where required due to legislative, operational or technological changes.

Adopted June 2026 to be reviewed annually in March.