Barrowby Parish Council

Email: clerk@barrowbyparishcouncil.gov.uk
Address: Reading Room, Church Street, Barrowby, NG32 1BX
Website: https://barrowby.parish.lincolnshire.gov.uk

IT / Email / Cyber Security Policy

Document control

- **Owner:** Full Council
- **Responsible officer:** Clerk / Proper Officer
- **Adopted:** 11.05.2026 (Minute ref: 8e [26/008])
- **Version:** 2025.1
- **Review:** Annually or earlier if legislation/guidance changes
- **Next review due:** January-March 2027 at Full Council for formal adoption at Parish Council May 2027

1. Purpose

This policy sets out the rules for the safe, lawful and appropriate use of Barrowby Parish Council's information technology, email, devices, systems and data.

The Council relies on information technology to deliver services, communicate with residents and partners, manage records, and protect confidential information. All users of Council systems must help maintain the security, integrity, availability and lawful handling of Council information.

This policy supports the Council's duties under the UK GDPR, the Data Protection Act 2018, the Freedom of Information Act 2000 and associated good practice in cyber security and records management.

2. Scope

This policy applies to all councillors, employees, contractors, volunteers, agency workers and anyone else authorised to access Council information or systems.

It applies to:

- Council email accounts;
- computers, laptops, tablets and mobile phones used for Council business;
- cloud storage, shared drives and software used for Council work;
- internet access and web-based systems;
- removable media such as USB devices;
- personal devices used for Council business where permitted.

3. Principles

The Council will manage IT and information in accordance with the following principles:

1. **Lawfulness and confidentiality** – information must be handled lawfully, fairly and securely.
2. **Security by default** – access, systems and devices must be protected by sensible, proportionate security controls.
3. **Least privilege** – users should only have access to the information and systems they need for their role.
4. **Human responsibility** – every user is responsible for protecting Council information and reporting concerns promptly.
5. **Retention and minimisation** – information must only be kept for as long as needed and in line with the Council's retention arrangements.
6. **Proportionate monitoring** – any monitoring must be lawful, transparent and proportionate.

4. Roles and responsibilities

4.1 Full Council

Full Council is responsible for approving this policy and supporting a culture of lawful and secure information handling.

4.2 Clerk / Proper Officer

The Clerk / Proper Officer is responsible for day-to-day implementation of this policy, including:

- allocating and removing access as appropriate;
- maintaining oversight of Council systems and accounts;
- ensuring incidents are logged and escalated appropriately;
- arranging backup, security and training arrangements;
- liaising with the Council's Data Protection Officer, IT support or other advisers where required.

4.3 All users

All users must:

- comply with this policy and related procedures;
- keep passwords and devices secure;
- use only approved systems for Council work;
- take care with emails, attachments and links;
- report loss, compromise, suspected phishing, misdirected emails, data breaches or other incidents immediately;

- complete required training.

5. Acceptable use

Council IT resources are provided primarily for Council business.

Limited personal use may be permitted where it is:

- lawful;
- reasonable and infrequent;
- does not interfere with Council duties;
- does not create security, reputational or storage risks; and
- does not breach this policy or any other Council policy.

Users must not use Council systems or accounts to:

- access, create, download, store or send unlawful, offensive, discriminatory, abusive or inappropriate material;
- harass, bully or intimidate others;
- infringe copyright, confidentiality or data protection requirements;
- carry out party-political campaigning in the name of the Council unless lawfully authorised;
- run personal businesses or private commercial activities;
- install or use unauthorised software, browser extensions, apps or cloud services.

6. Approved systems and software

Only approved systems, applications and storage locations may be used for Council business.

Council information must not be stored in personal email accounts, personal cloud storage, private messaging apps, or other unapproved services unless expressly authorised by the Clerk / Proper Officer for a specific purpose and appropriate safeguards are in place.

Users must not install software or change security settings on Council-managed devices unless authorised.

Where external platforms are used for Council business, they must be selected and used in a way that is proportionate, secure and legally compliant.

7. Access control and account security

7.1 User accounts

Each user must have their own account wherever reasonably possible. Shared accounts should be avoided unless there is a clear operational reason.

Access rights will be granted according to role and removed or amended promptly when duties change or access is no longer required.

7.2 Passwords

Users must create strong, unique passwords for Council accounts and must not reuse passwords from personal accounts.

Passwords must not be shared, written down insecurely, or sent by email or message.

If a password is suspected to be compromised, it must be changed immediately and reported to the Clerk / Proper Officer.

7.3 Multi-factor authentication

Multi-factor authentication must be enabled on Council email accounts and other Council systems wherever it is available and reasonably practicable, particularly where accounts provide access to sensitive information or administrative controls. NCSC recommends MFA, with stronger phishing-resistant methods preferred where available.

8. Devices, mobile working and personal devices

8.1 Council devices

Council devices must be kept secure and, where possible, protected by:

- password, PIN or biometric access;
- automatic screen locking;
- up-to-date software and security updates;
- antivirus / anti-malware protection where appropriate;
- encrypted storage where available.

8.2 Personal devices used for Council business

Where personal devices are used for Council business, the user must ensure that:

- the device is protected by a PIN, password or biometric login;
- the operating system and apps are kept up to date;
- Council information is accessed through approved accounts and services only;
- the device is not shared in a way that exposes Council information to other household members or third parties;
- lost or stolen devices used for Council work are reported immediately.

The Council may require Council information to be removed from a personal device where appropriate, for example when a user leaves office or ceases to require access.

8.3 Remote working

Users working remotely must take the same care with Council information as they would in a formal office environment. Screens should not be overlooked by others, paper records should be stored securely, and public or unsecured Wi-Fi should be avoided unless appropriate safeguards are in place. NCSC guidance specifically emphasises securing smartphones and tablets as part of basic cyber hygiene.

9. Email use

Council email accounts must be used professionally, respectfully and with care.

Users must:

- check the recipient list carefully before sending;
- take extra care when sending personal, confidential or sensitive information;
- use clear subject lines and professional language;
- be alert to phishing, spoofing, malicious attachments and suspicious links;
- report suspicious emails immediately;
- avoid forwarding chain messages, scams or irrelevant bulk emails.

Confidential or sensitive information must only be sent by approved secure means and only where necessary.

Email should not be used as a substitute for proper records management. Important Council decisions, records and correspondence must be retained in the appropriate system in accordance with the Council's retention arrangements. ICO guidance makes clear that retention periods must be justifiable and linked to purpose, rather than keeping data indefinitely.

9a Use of personal email accounts for Council business: Councillors should use a Council-provided email account for Council business wherever one is available.

Where a councillor exceptionally uses a personal email account for Council business, they must ensure that:

- the account is secured with a strong unique password and multi-factor authentication where available;
- Council emails are kept separate so far as reasonably practicable from personal correspondence;
- important Council emails, attachments and decisions are copied or forwarded promptly to the Council's official records system or Clerk / Proper Officer for retention and filing;

- personal email accounts are not used for storing confidential or sensitive Council information any longer than necessary;
- Council business is not conducted through another person's email account or through shared family access.

Councillors using personal email for Council business remain responsible for complying with data protection, freedom of information, lawful retention, confidentiality and this policy.

The Council may require relevant Council business records held in personal email accounts to be produced, transferred to Council systems, or deleted where appropriate and lawful.

10. Phishing, malware and unsafe content

Users must remain vigilant to cyber threats including phishing, malware, ransomware and fraud.

In particular, users must not:

- open attachments or click links from suspicious or unexpected emails;
- enable macros or downloads from untrusted sources;
- connect unknown USB devices to Council equipment;
- bypass security warnings without good reason.

Any suspected phishing email, malware infection, account compromise or fraudulent communication must be reported immediately. NCSC identifies backups, malware protection, phishing awareness, device security and keeping software updated as core cyber security steps for small organisations.

11. Data handling, storage and retention

Council information must be:

- accurate and kept up to date where necessary;
- stored in approved systems;
- accessible only to those who need it;
- retained only for as long as justified; and
- disposed of securely when no longer needed.

Special care must be taken with:

- personal data;
- special category data;
- staffing records;
- financial information;
- commercially sensitive or legally privileged material.

Users must follow the Council's privacy, records retention, FOI and breach reporting arrangements where applicable.

Paper records containing confidential information must be stored securely and disposed of through confidential waste arrangements or another approved secure disposal method. Digital records must be securely deleted when no longer required and when lawful to do so. ICO guidance notes that records awaiting destruction should also be stored securely.

12. Backups and business continuity

Important Council data must be backed up using approved arrangements.

The Council will ensure, so far as is proportionate to its size and systems, that:

- key records and data are backed up regularly;
- backups are protected from loss, unauthorised access and malware;
- the Council can restore important information if data is lost, corrupted or encrypted by ransomware.

NCSC identifies backing up data as a basic and essential security measure for small organisations.

13. Monitoring

The Council reserves the right to monitor the use of Council systems, accounts and devices where this is necessary for legitimate purposes such as:

- ensuring security and system integrity;
- investigating suspected misuse;
- meeting legal obligations;
- maintaining business continuity.

Any monitoring will be lawful, proportionate and carried out in line with data protection law. Covert monitoring will only be considered in exceptional circumstances, for a specific investigation, and with appropriate authority and assessment. ICO guidance states that worker monitoring should be transparent and proportionate, and covert monitoring should only be used exceptionally.

14. Security incidents and data breaches

A security incident includes, but is not limited to:

- a lost or stolen device;
- a hacked or suspected compromised account;
- a phishing attack;

- malware or ransomware infection;
- an email sent to the wrong recipient;
- unauthorised access to Council information;
- accidental deletion or disclosure of data.

All incidents and suspected incidents must be reported immediately to the Clerk / Proper Officer.

Where personal data may be affected, the incident must also be assessed under the Council's data breach procedure and escalated to the Data Protection Officer where appropriate. UK GDPR requires appropriate security measures and includes duties around personal data breach notification.

No user should attempt to hide an incident or "fix it quietly" without reporting it. Security incidents must be reported and handled in accordance with the Council's IT / Cyber Security Incident Report Procedure and, where personal data is involved, the Personal Data Breach Procedure. A brief incident record must be made for all reported incidents, even where no further action is ultimately required.

15. Leavers, role changes and return of information

When a councillor, employee, volunteer or contractor leaves office or no longer requires access:

- Council accounts and permissions must be reviewed and removed promptly;
- Council information held on personal devices or personal accounts must be returned, transferred or securely deleted as appropriate;
- any Council-owned equipment, documents, keys, tokens or storage media must be returned;
- shared passwords and recovery details must be changed where relevant.

16. Training and awareness

The Council will provide, or arrange access to, proportionate training and guidance on:

- cyber security awareness;
- phishing and email safety;
- data protection and confidentiality;
- records retention and secure handling of information;
- safe use of devices and remote working.

All users are expected to take reasonable steps to keep their knowledge up to date and to follow advice issued by the Council in response to changes in risk or guidance.

17. Non-compliance

Failure to comply with this policy may result in:

- removal or restriction of access to Council systems;
- internal action under the Council's relevant procedures;
- referral to the police, ICO or other authority where appropriate;
- contractual action in the case of contractors or service providers.

Any action taken will be proportionate to the seriousness of the breach.

18. Related policies and documents

This policy should be read alongside any relevant Council:

- Data Protection Policy;
- Privacy Notices;
- Records Retention / Document Retention Schedule;
- Data Breach / Personal Data Breach Procedure;
- Homeworking or Flexible Working arrangements;
- Social Media Policy;
- AI Use Policy;
- Staff disciplinary and code of conduct policies.
- IT / Cyber Security Incident Report Procedure;
- Personal Data Breach Procedure.
- Email Retention and Filing Protocol (Appendix 2)

19. Policy review

This policy will be reviewed at least annually, and sooner if required by:

- legislative change;
- ICO or NCSC guidance updates;
- significant changes to Council systems or working practices; or
- any serious incident or identified weakness.

20. Contact

Questions about this policy should be directed in the first instance to the Clerk / Proper Officer.

Where required, data protection matters will be referred to the Council's Data Protection Officer.

Appendix 1 – Minimum security standards for personal devices used for Council business

Where a personal device is used to access Council email, documents or systems, the following minimum standards apply:

1. **Access control**
   The device must be protected by a PIN, password or biometric login.
2. **Automatic locking**
   The device must be set to lock automatically after a reasonable period of inactivity.
3. **Updates**
   The operating system, browser and applications must be kept up to date with security updates applied promptly.
4. **Malware protection**
   Where appropriate to the device type, reputable antivirus / anti-malware protection must be installed and kept up to date.
5. **Secure accounts**
   Council accounts accessed on the device must use strong unique passwords and multi-factor authentication where available.
6. **Separate use**
   The device should not be shared in a way that allows other household members or third parties to access Council information.
7. **Secure storage**
   Council information should only be stored on the device where necessary and should otherwise be kept within approved Council systems or cloud services.
8. **Loss or theft**
   Any loss, theft or suspected compromise of the device must be reported immediately to the Clerk / Proper Officer.
9. **Public Wi-Fi**
   Public or unsecured Wi-Fi should be avoided when accessing sensitive Council information unless appropriate safeguards are in place.
10. **Deletion of Council data**
    When the device is replaced, disposed of, or no longer used for Council business, Council information must be securely removed where appropriate.

The Clerk / Proper Officer may issue additional practical guidance from time to time on the safe use of personal devices.

Appendix 2 – Email retention and filing protocol for the Clerk and councillors

The purpose of this protocol is to ensure that important Council emails are retained as Council records where necessary, while routine or duplicate emails are not kept longer than needed.

1. General rule

Emails are Council records if they contain:

- decisions or actions of the Council;
- formal instructions, approvals or authorisations;
- substantive advice or information relied upon by the Council;
- correspondence relating to contracts, staffing, finance, complaints, legal matters, FOI requests, data protection matters or statutory functions;
- records needed for audit, accountability or business continuity.

Routine, trivial, duplicated or transitory emails should not be retained longer than necessary.

2. Clerk responsibilities

The Clerk / Proper Officer should:

- ensure important Council emails are saved in the appropriate Council filing system or folder structure;
- retain emails in line with the Council's retention arrangements;
- avoid relying solely on inbox storage as the record system;
- ensure important attachments are saved with the related record where needed;
- organise folders so that records can be located efficiently if required.

3. Councillor responsibilities

Councillors should:

- keep Council emails separate from personal correspondence where reasonably practicable;
- forward or copy important Council emails to the Clerk / Proper Officer where they form part of the Council's formal record;
- delete duplicated, trivial or purely administrative emails when no longer needed;
- not retain Council emails indefinitely in personal inboxes.

4. Personal email accounts

Where councillors use a personal email account for Council business, important emails must be copied or forwarded to the Council's official record system or the Clerk / Proper Officer as soon as reasonably practicable.

5. Sensitive material

Emails containing confidential, personal, staffing, legal or sensitive information must be handled with particular care and retained only in appropriate secure locations.

6. Deletion

Emails should only be deleted where this is consistent with the Council's retention arrangements, legal obligations and any ongoing complaint, audit, FOI request, subject access request, litigation or investigation.