

WHITTINGHAM, CALLALY AND ALNHAM PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

Purpose of the IT Policy	2
Scope of this policy	2
Computer use and equipment	2
Portable equipment	2
Use of own devices	3
Health and safety	3
Password and authentication policy	4
Remote working	4
Email	5
Use of the Internet	5
Website and social media	5
Use of artificial intelligence and automated tools	6
Security incidents and data breaches	6
Misuse	6
Review	6
Important notice	6

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

This policy has been adapted from the NALC model to reflect the Council's small-scale, home-based working arrangements. It applies to Council-owned and personal equipment used for Council business.

Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided or authorised by the Council.

Computer use and equipment

- 3.1** Council computer equipment is provided for Council purposes only.
- 3.2** All councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all Council and personal devices used for work.
- 3.3** All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the Council.
- 3.4** Councillors, staff, and other authorised users are not to purchase any computer or mobile equipment, including software, unless previously authorised.
- 3.5** Personal disks, USB sticks, CDs, DVDs and other data storage devices cannot be used on Council computers without the prior approval of the Clerk.
- 3.6** Any faults, loss, damage or necessary repairs must be reported to the Clerk.

Portable equipment

- 4.1** Council back-up procedures specific to portable equipment should be followed at all times.
- 4.2** All portable computers must be stored safely and securely when not in use. Portable equipment should not be left unattended away from home or Council premises and should never be left visible in parked vehicles.
- 4.3** It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold Council data, including emails and files, must be protected with a PIN code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disabled or removed.

4.4 Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods, for example, entering a password and confirming a code sent to a mobile device. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

Use of own devices

The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets or laptops to access Council email, documents, cloud storage or other services for normal Council purposes. Any such use of personal devices will be at the discretion of the Council. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software are appropriately patched or updated.

5.1 The same security precautions apply to personal devices as to Council equipment.

5.2 Wherever possible the user should maintain a clear separation between the personal data processed on the Council's behalf and that processed for their own personal use, for example, by using different apps or profiles for Council and personal use.

5.3 Users must protect their devices with a strong password, PIN, fingerprint or other secure method and configure them to lock automatically after a period of inactivity.

5.4 Users must ensure secure Wi-Fi networks are used and that work-related data cannot be viewed or retrieved by family or friends who may use the device.

5.5 Users must inform the Clerk if a device is lost, stolen or inappropriately accessed where there is a risk of access to Council data or resources.

5.6 Any work done on a user's own equipment should be stored securely and password protected and should always be backed up in accordance with the Council's standard back-up procedures.

5.7 Prior to the disposal of any device that has Council data stored on it, and when a user leaves the Council, all Council data, saved passwords and access shortcuts must be securely removed after any official records have been transferred to the Council.

Health and safety

6.1 The Council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment.

6.2 Any employee who feels that their workstation requires changes to make it compliant must speak to the Council.

6.3 If any hazards are detected at a workstation, including unusual noises from IT equipment, this should be reported immediately to the Clerk or Chair.

Password and authentication policy

All user accounts must be protected by strong, secure passwords. The Council follows the National Cyber Security Centre (NCSC) recommendation for creating passwords using three random words. This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks.

7.1 Multi-Factor Authentication should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification, for example, a password and a code sent to a phone. This significantly reduces the risk of unauthorised access to systems and personal data.

7.2 Default passwords provided by vendors or service providers must be changed immediately upon installation or setup.

7.3 Passwords are personal and must not be shared under normal circumstances. In exceptional cases, access to administrative or system credentials may be granted through an authorised and secure recovery arrangement.

7.4 Passwords must not be stored in plain text or written down in insecure locations. Where passwords must be recorded for continuity, they must be stored using a Council-approved encrypted password manager or another secure arrangement approved by the Council.

7.5 Passwords must be changed immediately if compromise is suspected.

7.6 Users are responsible for creating and maintaining secure passwords for their accounts.

Remote working

Increased IT security measures apply to those who work away from their normal place of work, including whilst travelling, working from home, attending meetings or working at another venue, as follows:

8.1 Council services should not be accessed using computers that do not belong to the Council or the user. Passwords must not be saved on any shared or public device.

8.2 The location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport.

8.3 Any data printed should be collected and stored securely.

8.4 Papers, files or computer equipment must not be left unattended unless they are kept in a locked room, cabinet or other secure location.

8.5 Any data should be kept safely and should only be disposed of securely.

8.6 Papers, files and portable storage should not be left unattended in cars. If this is entirely unavoidable for a short period, they must be locked out of sight.

8.7 Where possible, the ability to remotely wipe mobile devices that process sensitive information should be retained in case of loss or theft.

Email

Council email facilities are intended to promote effective and speedy communication on work-related matters. Although the Council encourages the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto Council systems and should take proper account of the security requirements in this policy.

9.1 Council business must be conducted through email accounts authorised by the Council. In line with proper practices, the Council will maintain a generic email account hosted on a Council-owned domain and will move towards providing individual Council-domain email accounts where required.

9.2 Email messages sent on a Council account are for Council use only. Personal use is not permitted.

9.3 Users should check senders, recipients, links, attachments and requests for payments or changes to account details before acting. Suspected phishing or fraud must be reported to the Clerk.

9.4 Personal or sensitive data should only be sent where necessary and by an appropriately secure method, in accordance with the Council's Data Protection Policy.

9.5 If there is something not covered in this policy, councillors, staff, and other authorised users should ask the Clerk rather than assuming they know the right answer.

Use of the Internet

10.1 It is easy to copy electronically, but this does not make it any less an offence. The Council's policy is to comply with copyright laws, and not to bend the rules in any way.

10.2 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. Copyright conditions should be checked before downloading, copying or publishing material.

10.3 The Council does not permit the registration of any new domain names relating to the Council's name unless authorised to do so. Links must not be added to the Council's website without the approval of the Clerk.

10.4 Special rules apply to the processing of personal and sensitive personal data. Further guidance is contained in the Council's Data Protection Policy.

10.5 Be aware that, as the Internet is uncontrolled, much of the information available may be less accurate than it appears.

Website and social media

11.1 Comments posted by councillors, staff, and other authorised users on Council sites should be knowledgeable, accurate and professional and should not compromise the Council in any way.

11.2 Details relating to events, conversations, materials or documents that are private, confidential or internal to the Council should not be posted. This does not affect statutory requirements to publish information, including under the Freedom of Information Act.

11.3 Postings to websites, the internet, social media, press or other media should not breach copyright or other law, disclose confidential information, defame any person or disclose personal data in breach of data protection legislation.

11.4 Contacts from the media relating to the Council should be referred to the Clerk.

11.5 Council account details remain the property of the Council. Councillors, staff, and other authorised users leaving the Council will be required to return or delete all Council-related data from personal devices or equipment after transferring the official record to the Council.

Use of artificial intelligence and automated tools

This section has been added to address technology not covered expressly in the NALC model.

12.1 Personal data, confidential information, unpublished legal advice, security information and account credentials must not be entered into an AI or automated service unless the service has been specifically approved for that purpose and its data-handling arrangements are suitable.

12.2 AI-generated material must be checked by a responsible person for accuracy, bias, confidentiality, copyright and legal or procedural errors before it is relied upon or published.

12.3 AI tools may assist administrative work but must not make Council decisions, exercise delegated authority or replace the judgement and accountability of the Council, Clerk or councillors.

Security incidents and data breaches

Any loss, theft, unauthorised access, malware, phishing, compromised account or other suspected security incident must be reported to the Clerk immediately. The Clerk will take appropriate steps to contain and record the incident and assess whether it must be reported to the Council, Information Commissioner's Office, insurer, bank, police or affected individuals.

Misuse

Misuse of IT systems and equipment is not in line with the Council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action. This may include withdrawal of access, disciplinary proceedings for an employee, referral under the Code of Conduct where applicable, recovery of loss or referral to the relevant authority.

Review

This policy will be reviewed annually and following any significant security incident, change in legislation or material change to the Council's systems or working arrangements.

Important notice

This is an example of a policy designed for a small Council adhering to statutory minimum requirements and does not constitute legal advice. As with all policies it should be consistent with the Council's terms and conditions of employment. This document was commissioned by the National Association of Local Councils (NALC) for the purpose of its member councils and county associations. Every effort has been made to ensure that the contents of the model are correct at time of publication. NALC cannot accept responsibility for errors, omissions and changes to information subsequent to publication.