Nettleham
Parish Council

IT POLICY

Nettleham Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

Scope

This policy applies to:

All staff and Councillors, working on behalf of the Council.

All devices and services used for Council business, including:

Council-owned computers, tablets, phones, and shared office equipment.

Personally owned devices used to conduct Council work (BYOD)

All communications platforms: email, internet, messaging, website, and social media.

Closed Circuit Television (CCTV)

Related Policies

This policy must be read in conjunction with:

- Data Protection Policy
  GDPR Privacy Policy
  Disciplinary Rules (for staff)
  Councillor Code of Conduct
  Equality and Diversity Policy

Equipment and Device Use

All staff and Councillors may use either Council-owned devices and IT systems, or personally owned equipment (BYOD), subject to minimum standards

All devices used for Council business must:

Be protected with a password or screen lock.

Be updated with security patches and protected from malware.

Store files in backed-up systems.

Adopted 18th November 2026
Review Date: November 2027

Where personally owned devices are shared with others (e.g. family members), access to Council information must be restricted to a secure, password-protected user account or profile that is used exclusively by the Councillor or staff member.

Lost or compromised devices must be reported immediately to the Clerk. Devices should not be left unattended in public spaces.

Email Communication

All Council business must be conducted using nettleham-pc.gov.uk email addresses.

Personal accounts must not be used to store, send, or receive Council-related communications.

Messages should be clear, factual, courteous and suitable for formal records.

Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Nettleham Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

Email Communication – Multiple Recipients

Protecting Privacy

Using BCC in Outlook ensures that the email addresses of all recipients are hidden from one

another. This is particularly important when sharing personal email addresses, as it prevents exposure to spam, phishing, or unauthorised sharing.

Avoiding Unintended Reply-All

When you BCC recipients in Outlook, you minimise the risk of recipients using the “Reply All” function, which can lead to cluttered inboxes and potential breaches of privacy if sensitive information is shared.

Internet and Software Use

Limited personal internet use is allowed on breaks if it does not interfere with Council business or security.

All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

The following are strictly prohibited:

- Accessing offensive, discriminatory or illegal content on Council owned devices or using Council provided internet connections.
- Using Council devices for gambling or streaming.
- Downloading or installing software on Council owned devices without authorisation
- Accessing chat rooms, anonymous messaging services, or unapproved blogs from Council systems.

Social Media and Website Use

Council Website and Social Media Channels

The Clerk has overall responsibility for content on the Council's website and official social media accounts. This responsibility may be delegated to another officer, who will act under the Clerk's direction. All official posts and responses on behalf of the Council must be consistent with agreed Council positions.

The Council website is the official platform for publishing agendas, minutes, contact details, policies, statutory notices, and community information. No unofficial website may represent or impersonate the Council.

Use of Social Media by Councillors

Councillors must adhere to the Councillor Code of Conduct in all online activity, including posts made from personal accounts.

Councillors should:

- Distinguish clearly between personal views and Council policy.
- Avoid commenting on live or sensitive Council matters that are not yet public or agreed.
- Refrain from posting anything that could be considered defamatory, discriminatory, confidential, or likely to damage public confidence in the Council.
- Not pre-determine planning or regulatory issues through public comment.
- Never share confidential data or information acquired in their official capacity.
- Breaches of this section may result in referral to the Monitoring Officer.

Data Protection and Privacy

All devices and systems used for Council work must handle personal data in line with GDPR and the Council's GDPR Policy. Staff and Councillors must:

Access data only for legitimate reasons.

Store files securely.

Avoid unauthorised disclosure or copying of personal information.

Report suspected breaches immediately to the Clerk.

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

Passwords and Access

Users are responsible for maintaining the security of their accounts and passwords:

Passwords must be kept private and changed periodically.

Users must log out or lock devices when unattended.

No one should access another user's accounts or data without permission.

No one should attempt to discover or use another person's password.

If a password is compromised, users must notify the Clerk immediately.

Access to another user's account or data may only occur with permission or when authorised for business continuity (e.g., during absence).

Where password-protected documents are sent by email, the password should be communicated separately.

Safe Use and Security Guidance

Devices should be shut down after use each day.

Files should be saved to shared drives or secure cloud systems, not just local storage.

Public Wi-Fi should be avoided for sensitive work unless using a secure connection (e.g., VPN)

Extra precautions must be taken when working in public areas to avoid unauthorised viewing of Council information.

Mobile Messaging and Texts

Messages sent via SMS, or other platforms for Council business must be professional and factual.

As with emails, texts may be disclosable under FOI or data protection law.

Avoid emojis, slang or ambiguity in official communications.

Mobile devices provided by Nettleham Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

CCTV Use

The Council operates Closed Circuit Television (CCTV) at its premises for the purposes of:

- Enhancing the safety and security of staff, Councillors, visitors, and members of the public.
- Protecting Council property and assets
- Preventing and detecting crime or antisocial behaviour
- Assisting in the investigation of incidents or complaints

Legal Basis and Data Protection

CCTV recordings constitute personal data under the UK GDPR.

The Council has a legitimate interest in using CCTV for security and safety, provided it is done in a proportionate and transparent manner.

Appropriate signage is displayed to inform individuals of CCTV surveillance.

Recorded footage is stored securely and access is limited to authorised personnel only.

Access and Disclosure

CCTV footage will only be viewed by authorised officers and may be disclosed to law enforcement or insurers where appropriate.

Individuals may request access to their personal data captured by CCTV, subject to verification and lawful exemptions.

All disclosures must be approved by the Clerk or their designated officer

Retention and Disposal

CCTV footage is retained for a limited period (normally no longer than 30 days), unless required for a specific investigation.

Recordings are securely deleted when no longer required.

Review and Oversight

The Clerk is responsible for ensuring that CCTV is operated in compliance with this policy and relevant data protection legislation.

The Council's use of CCTV is subject to periodic review to ensure its continued necessity and proportionality

Monitoring and Oversight

The Clerk is responsible for overseeing this policy and investigating misuse.
The Council reserves the right to access Council-issued devices and data if required for operational, legal, or disciplinary purposes. All staff and Councillors are informed through this policy that such monitoring may occur.
Any such access will be proportionate and necessary.

14. Misuse and Disciplinary Action

Misuse includes:

- Using Council systems for unlawful or offensive content.
- Disclosing confidential or personal data without consent.
- Misrepresenting the Council online
- Installing unapproved software or bypassing security
- Attempting to discover or share another user's password.
- Circumventing or disabling network security.
- Leaving laptops or devices unattended in public places.

Consequences may include disciplinary action, loss of access to Council systems, or referral under the Councillor Code of Conduct.

Policy Review and Training

This policy will be reviewed annually or following significant changes to law, guidance, or systems.
Guidance will be provided at induction, regularly when responsibilities or systems change and .
All staff and councillors are responsible for the safety and security of Immingham Town Council's IT and email systems. By adhering to this IT Policy Nettleham Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.