Information and Communications Technology (ICT) Policy 2025-29

STATEMENT OF PURPOSE

The purpose of this policy is to ensure that all employees, volunteers, contractors, and Members using Felixstowe Town Council IT have a clear understanding of what is and is not permitted. This ensures appropriate use of council equipment, safeguards the security of its IT systems and data, and assists compliance with UK Data Protection law, the UK GDPR, and other relevant legislation.

This policy should be read alongside:

- **Data Retention Policy:** Link
- **Press and Media Policy:** Link
- **Data Protection Policy:** Link

Members are also encouraged to review the latest **NALC Good Councillors Guide to Cyber Security**: NALC Guide

A glossary of ICT terminology can be found at: **ICT Glossary**

SCOPE

This policy covers the security and use of all Felixstowe Town Council information and IT equipment, including email, internet, voice, mobile devices, and cloud-based systems. It applies to all employees, Members, contractors, volunteers, and other users of council IT systems.
It applies to all council information, regardless of format, including information relating to other organisations or individuals with whom the council interacts. It also covers all IT and communications facilities operated by the council or on its behalf.

COMPUTER SECURITY CONTROL

Access to the council's IT systems must be controlled by robust security protocols, including unique user IDs, strong passwords, and, where available, Multi-Factor Authentication (MFA). Users are accountable for all actions on council IT systems.

Users must not:

- Leave accounts logged in on unattended or unlocked devices
- Leave passwords unprotected or share them
- Make unauthorised changes to IT systems or data
- Attempt to access data they are not authorised to use
- Connect unauthorised devices or store council data on personal equipment
- Share council data externally without appropriate authority

Line managers must provide clear guidance on limits of authority regarding IT systems and data.
Personal files (music, video, games, etc.) must not be stored on council equipment.

ACCEPTABLE USAGE POLICY

Internet and Email

Council IT systems are primarily for business use. Limited personal use is permitted provided it does not affect performance, contravene any law, or breach council policies.

Unacceptable Internet Behaviour Includes:

- Visiting illegal, obscene, pornographic, or hateful sites
- Fraud, software or media piracy
- Harassment or offensive messaging
- Hacking or unauthorised access
- Publishing defamatory or confidential information
- Deliberate waste of resources or introducing malware

Unacceptable Email Behaviour Includes:

- Sending or storing illegal, offensive, or discriminatory content
- Conducting private business or chain letters
- Forwarding confidential messages externally
- Violating copyright law
- Introducing viruses or malware

Good Practice:

- Regularly archive or delete emails in line with the Data Retention Policy
- Be aware of phishing/spam and report suspicious emails to IT support
- All council emails must include an appropriate disclaimer linking to the Council's Privacy Policy

COUNCIL INFORMATION ON THIRD-PARTY SERVICES

Council data stored on third-party services, including social media and cloud platforms, remains the property of Felixstowe Town Council. Council information should only be stored on approved cloud services (e.g., Office 365/SharePoint) under council contracts.

CLEAR DESK AND CLEAR SCREEN

- Lock or log off devices when unattended
- Protect confidential documents, including on printers and photocopiers
- Dispose of sensitive material securely (cross-cut shredders)

SOFTWARE AND VIRUSES

- Only council-authorised software may be used, in compliance with licensing agreements
- Software must be regularly updated and supported
- Antivirus protection must not be disabled; infections must be addressed via approved procedures

TELEPHONY EQUIPMENT

Council voice systems are for business use. Limited personal use is permitted if it does not affect work performance. Users must not:

- Conduct private business
- Make hoax or threatening calls
- Accept reverse charge calls unless for business purposes

LEAVING THE COUNCIL

All council equipment and data must be returned at the end of employment or office term. Council data and intellectual property remain council property.

MONITORING AND FILTERING

The council may monitor ICT systems, including email and internet use, to ensure security and compliance. Monitoring is in line with:

- UK Data Protection law and GDPR
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000

Breaches may result in disciplinary action or, for Members, Code of Conduct investigations.

MOBILE DEVICES AND BRING YOUR OWN DEVICE (BYOD)

This applies to all council-issued and personal devices accessing council information.

Responsibilities:

- Protect council information and devices
- Store council information only as necessary and delete when no longer needed
- Keep devices updated and secure
- Ensure compliance with Data Protection law

Device Security:

- Strong passcodes, passwords, or biometrics
- Automatic lock within 5 minutes of inactivity
- Encryption for sensitive or personal data

Remote Work & Travel:

- Secure connections (VPN) should be used when working remotely
- Overseas use must be approved due to potential costs and security risks

Termination / Device Replacement:

- All council information must be deleted from personal or issued devices upon leaving or replacing the device
- Council reserves the right to inspect, remove, or wipe data to protect council information

REMOVABLE MEDIA

- Only use council-authorised removable media for confidential data, encrypted to AES 256 or equivalent
- Media should be physically protected, and data securely deleted when no longer required

WIRELESS INTERNET

- Public Wi-Fi access for Town Hall hirers is provided under terms of acceptable usage
- Public network is segregated from council systems for security

POLICY REVIEW

This policy will be reviewed at least every four years or sooner if legislative, technological, or operational changes require updates.