Information and Communications Technology (ICT) Policy 2026-2030

1. STATEMENT OF PURPOSE

The purpose of this policy is to ensure that all employees, volunteers, contractors, and Members have a clear understanding of their responsibilities when using Felixstowe Town Council's digital infrastructure. This policy ensures the appropriate use of equipment, safeguards the security of systems and data, and ensures compliance with UK Data Protection law, the UK GDPR, and the JPAG Practitioners' Guide 2025.

This policy should be read alongside:

- Data Retention Policy
- Data Protection Policy
- Press and Media Policy

Members are also encouraged to read the NALC Good Councillors Guide to Cyber Security

2. SCOPE

This policy applies to all Council-owned equipment and any personal devices used to access Council data (Bring Your Own Device - BYOD). It covers email, internet, voice, mobile devices, and cloud-based systems (e.g., Microsoft 365).

3. DIGITAL IDENTITY & SECURITY (Audit Compliance)

To satisfy the requirements for secure identity and data integrity:

- **Official .gov.uk Use:** To meet technical standards (JPAG Guide Para 1.47), all Council business must be conducted via official @felixstowe.gov.uk email accounts. This ensures a clear separation between personal and authority data.
- **Multi-Factor Authentication (MFA):** The use of MFA is required for all users accessing Council cloud services and remote systems to protect against unauthorised access.
- **Access Control:** Access to IT systems is controlled via unique user IDs. Users are responsible for the security of their login credentials and must not share passwords.

4. WEBSITE ACCESSIBILITY (WCAG 2.2)

To comply with the 2018 Regulations and JPAG Guide Para 1.49, the Council is committed to a website that meets WCAG 2.2 AA standards:

- **Internal Content:** All digital documents produced by the Council (Agendas, Minutes, Reports) must be created as "Native PDFs" (saved directly from Word/Excel).
- **Third-Party Content:** The Council frequently publishes documents provided by external bodies (e.g., Planning Applications, Grant evidence, or Community posters). These are exempt from the accessibility regulations under the 'Third-Party Content' clause as they are neither funded nor developed by the Council. The Council will provide a contact point on the website for residents to request assistance with these documents.
- **Documented Reviews:** The Council will maintain a record of manual accessibility testing to provide evidence of ongoing compliance.

5. MOBILE DEVICES AND BRING YOUR OWN DEVICE (BYOD)

- **Auto-Lock:** Devices used for Council business must be configured to automatically lock within 5 minutes of inactivity.
- **Security Updates:** Users are encouraged to ensure critical security patches are installed on personal devices promptly (ideally within 14 days of release).
- **Incident Reporting:** Users must report the loss of any device accessing Council data, or any suspected data breach (such as clicking a suspicious link), to the Town Clerk immediately.
- **Data Removal:** Upon leaving the Council or replacing a device, all Council information must be deleted. The Council reserves the right to remove Council-owned data to protect the authority's information.

6. 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

7. 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

8. ACCEPTABLE USAGE

- **Usage:** Council IT systems are for business use. Personal use must be limited and must not interfere with work performance or breach Council policies.
- **AI Usage:** Staff may use AI tools to assist with drafting and research, provided that no personal or confidential data is entered into the tool and all output is verified for accuracy.

- **Software:** Only software authorised and licensed by the Council may be installed on Council equipment. Users must not download or install unauthorised software, browser extensions, or applications.
- **Monitoring:** The Council reserves the right to monitor ICT systems, including email and internet use, to ensure security and compliance with the law.

9. COMPLIANCE & AWARENESS

- **Awareness:** The Council will provide regular security briefings and guidance. All users are expected to maintain an awareness of current cyber risks (such as phishing).
- **Statement of Understanding:** Upon adoption of this policy, Members and Staff will be asked to sign a Statement of Understanding. This serves as the Council's primary evidence for the Internal Auditor that users are aware of their responsibilities regarding MFA and data security.

10. POLICY REVIEW

This policy will be reviewed on a four-year cycle or sooner if required by changes in legislation (specifically the JPAG Practitioners' Guide) or technology.