Edwinstowe Parish Council IT Policy

1. **Purpose**
   This IT Policy provides a framework for the effective, secure and responsible use of information technology systems within Edwinstowe Parish Council.

   The policy ensures that the council:
   - protects its information and IT systems
   - manages digital communication responsibly
   - complies with relevant legislation including the UK General Data Protection Regulation and the Data Protection Act 2018
   - follows best practice guidance issued by the National Association of Local Councils

   The Clerk to the Council is responsible for the day-to-day administration of council IT systems.

2. **Scope This policy applies to:**
   - all councillors, employees, contractors and volunteers
   - any device used to access council information or systems
   - council email accounts, website systems and official social media platforms

   This includes both council-owned devices and personal devices used for council business.

3. **Acceptable Use of IT Systems**
   Council IT systems must be used responsibly and primarily for official council business.
   Users must:

   - act professionally when using council systems
   - not access, download or distribute illegal, offensive or inappropriate material
   - keep login details confidential
   - log out of systems and lock devices when not in use

   Limited personal use may occur where it does not interfere with council business and does not breach this policy.

4. **Council Email and Digital Communications**
   Council business should be conducted using official council email accounts where possible.

Councillors and officers should:

- use council email addresses for official communications where available
- avoid using personal email accounts for council business where possible
- ensure communications are professional and appropriate
- comply with the council's Code of Conduct

Care must be taken when sending confidential or personal information. Sensitive information should only be shared where necessary and using secure methods where appropriate.

5. **Data Protection and Information Security**
   Edwinstowe Parish Council is committed to protecting personal data and handling information responsibly.
   All users must:
   - only collect or process personal data where necessary for council business
   - ensure personal data is stored securely
   - avoid unnecessary sharing of personal information
   - follow the council's privacy notices and data protection procedures

   Any suspected data breach or loss of personal data must be reported immediately to the Clerk.

6. **Device Security**
   Devices used for council business must meet minimum security standards. These include:
   - password protection
   - screen locking when unattended
   - up-to-date operating systems and software
   - appropriate security software where required

   Users should avoid accessing council systems through unsecured public Wi-Fi networks where possible.

7. **Hardware and Software**
   Council equipment must be used responsibly.
   - Only authorised software may be installed on council-owned devices.
   - Hardware assets should be recorded and periodically reviewed.
   - Personal devices used for council work must be kept secure and comply with this policy.

8. **Cloud Storage and File Sharing**
   Council files may be stored electronically using approved storage systems.
   Users should:
   - only store council information on authorised systems
   - avoid storing council files on personal accounts where possible
   - ensure documents containing personal data are appropriately protected

9. **Backup and Data Recovery**
   Important council information should be backed up regularly.
   Backups should:
   - be stored securely
   - allow information to be recovered in the event of data loss, cyber incident or hardware failure

10. **Cyber Security Awareness**
    Users should remain alert to cyber security risks including:
    - phishing emails
    - suspicious attachments or links
    - fraudulent communications

    Any suspicious activity or cyber incident should be reported to the Clerk immediately.

11. **Website and Social Media**
    Only authorised individuals may update the council website or post on official council social media accounts.
    Content must:
    - be accurate and appropriate
    - reflect the council's role and responsibilities
    - comply with legal and data protection requirements

    Personal views must not be presented as the official position of the council.

12. **Monitoring and Compliance**
    The council reserves the right to monitor the use of its IT systems where necessary to ensure compliance with this policy and relevant legislation.

    Failure to follow this policy may result in removal of access to council systems or other appropriate action.

13. **Training**

    Councillors and staff may receive training relating to:

    - cyber security awareness
    - data protection and information governance
    - responsible use of digital systems

14. **Policy Review**

    This policy will be reviewed annually or sooner if required due to legislative or operational changes.

The IT Policy has been updated to better align with current guidance issued by the National Association of Local Councils and to support the council's governance requirements under the Annual Governance and Accountability Return, including the new digital governance expectations in Asser on 10.

The revisions do not significantly change the intent of the original policy but provide additional clarity and strengthen areas that auditors are now expecting councils to address. These include clearer guidance on the use of council email accounts, device security, cyber-security awareness, cloud storage of council information, and the reporting of data breaches or cyber incidents.

The policy review period has also been updated to annual review, which reflects current good governance practice. Overall, the amendments ensure the council's IT arrangements are clearly documented and consistent with national guidance.

Adopted by Full Council on 13th May 2026, Minute Reference 26/007