Essington Parish Council – Information Technology (IT) and Email Policy

Based on the NALC Model IT Policy Template (December 2025)
Effective Date: *March 2026* **Review Date:** *Annually*

1. Purpose

This policy sets out how Essington Parish Council's councillors, staff, and authorised users must use council IT systems, equipment, software, and email accounts in a **secure, lawful, and responsible manner**, in line with NALC's recommended governance standards.

The aims of this policy are to:

- Protect the council's digital assets and data.
- Set expectations for acceptable use of IT systems.
- Reduce risks related to cybersecurity, data loss, and misuse.
- Comply with GDPR, the Data Protection Act 2018, and the Practitioners' Guide 2025.

2. Scope

This policy applies to:

- All councillors, employees, volunteers, and contractors using council IT resources.
- All council-owned and personal devices used to conduct council business (BYOD).

IT resources include computers, tablets, smartphones, networks, cloud storage, software, and all council email accounts.

3. Acceptable Use

Users must:

- Use IT systems **primarily for council business**. Limited personal use is permitted if it does not interfere with duties.
- Follow ethical standards and obey copyright law.
- Avoid any offensive, illegal, or inappropriate content.

Monitoring may occur **where legitimate**, proportionate, and in accordance with privacy and data-protection laws.

4. Email Policy

4.1 Official Email Requirement

In accordance with NALC and GDS guidance, **all councillors and staff MUST use council-owned, role-based email addresses** for all council business.
Examples:

- clerk@essingtonparishcouncil.gov.uk
- chair@essingtonparishcouncil.gov.uk

This ensures professionalism, improves GDPR compliance, and avoids risks associated with personal email accounts.

4.2 Prohibited Use

- **Personal email accounts must not be used** for council business under any circumstances.

4.3 Email Content & Conduct

Users must:

- Maintain professionalism and clarity in communications.
- Encrypt sensitive or confidential data before sending.
- Be cautious about attachments and links to avoid phishing.

4.4 Continuity

Role-based accounts ensure access continuity during staff or councillor changes.

5. Domain & Website Standards

The council will operate on a **.gov.uk domain** for email and website hosting, following NALC and GDS recommendations supporting trust, security, and accessibility compliance.

The council website must meet WCAG 2.2 AA accessibility standards.

6. Hardware, Software & Device Management

6.1 Council-Owned Equipment

Users must:

- Treat equipment responsibly and avoid food/drink risks.
- Keep devices secured when unattended.
- Report faults to the Clerk immediately.

6.2 Software

- Only authorised software may be installed.
- Users may not bypass security settings or reinstall/dismantle devices.

6.3 Portable & Mobile Devices

Portable devices (laptops, tablets, smartphones):

- Must be encrypted and protected with PIN/biometrics.
- Must not be left unattended or stored in vehicles.
- Should be kept close to the user when out of the office.

7. Bring Your Own Device (BYOD)

Personal devices may be used **only if**:

- The device is secure, updated, and protected by strong passwords.
- Council data is stored solely in approved, secure council systems (never locally).
- The device has up-to-date antivirus software.

If a device is lost, stolen, or compromised, it must be reported immediately.

8. Password & Account Security

Users must:

- Use strong, unique passwords containing upper/lowercase letters, numbers, and symbols.
- Never reuse passwords across accounts.
- Change passwords periodically.
- Keep passwords confidential and never share them.

Two-factor authentication should be enabled wherever possible.

9. Data Management & GDPR

The council is a Data Controller under UK GDPR. All personal data must be:

- Collected, stored, processed, and deleted securely.
- Accessed only when necessary for council business.
- Stored only on approved systems with appropriate backups.

Backups must follow council procedures and be stored securely both onsite and/or cloud-based.

Data breaches must be reported to the Clerk immediately for potential ICO notification within 72 hours.

10. Network & Internet Use

- Internet access must be used responsibly for council purposes.
- Downloading or sharing copyrighted content without authorisation is prohibited.

11. Monitoring

The council may monitor IT and email use for:

- Safeguarding
- Compliance
- Security
- Legal requirements

Monitoring will always be proportionate and in accordance with GDPR.

12. Retention & Archiving

Email and electronic records must be archived according to legal, regulatory, and GDPR requirements.
Old or unnecessary emails should be regularly deleted.

Official council accounts ensure ease of FOI and Subject Access Requests.

13. Reporting IT Incidents

All suspected:

- Security breaches
- Phishing attempts
- Data loss
- Device theft
  must be reported immediately to the Clerk.

14. Training & Awareness

The council will provide ongoing training on:

- Cybersecurity
- Email safety
- IT best practices

- Data protection legislation

This is required under NALC-aligned governance standards.

15. Compliance & Consequences

Failure to comply with this policy may result in:

- Suspension of IT access
- Disciplinary action
- Referral to relevant authorities where appropriate

16. Contacts

For IT matters, contact:
Clerk & Proper Officer
Email: clerk@essingtonparishcouncil.gov.uk