IT and ICT Security Policy

Author	Amended	Adopted	Summary of amendments
Ross Gurney		194/25 Full council	➢ Policy adopted

56 Church Road, Tiptree, CO5 0SU
01621 817030
clerk@tiptreeparishcouncil.gov.uk
www.tiptreeparishcouncil.gov.uk

Contents

1. Aim of the Policy

The aim of this policy is to protect Tiptree Parish Council's information, data, and ICT communication systems. The Council recognises that effective information security is essential to good governance and public confidence.

This policy is aligned with guidance and best practice issued by the National Association of Local Councils (NALC), the Society of Local Council Clerks (SLCC), and the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

(Aligned with NALC and SLCC model guidance and best practice)

The policy seeks to reduce the risk of:

- **Data leaks and unauthorised disclosure of information**
- **Loss, corruption, or unavailability of communications and records**
- **Regulatory or statutory non-compliance**
- **Cyber security threats, including malware, phishing, ransomware, and hacking**

2. Scope

This policy applies to:

- **All Parish Councillors**
- **All employees of Tiptree Parish Council**
- **Any contractors or volunteers who access Council ICT systems or data**

3. ICT Systems and Council Email Accounts

- **All staff and councillors will be provided with a Council-owned gov.uk email account.**
- **All official Council business must be conducted using Council-provided email accounts.**
- **Personal email accounts must not be used for official Council work under any circumstances.**
- **Council email accounts are subject to monitoring and auditing where necessary for legal, security, or operational reasons.**

4. Data Protection and GDPR Compliance

- **All users must handle personal data in accordance with UK GDPR principles.**
- **Personal data must only be accessed where necessary for Council duties.**
- **Data must not be shared with unauthorised individuals or organisations.**
- **Council information must not be downloaded, copied, or stored on unauthorised devices or systems.**

5. Use of Personal Devices

- **Accessing Council email or systems from a personal device is permitted as long as precautions are taken.**
- **When accessing council data from a personal device the person is responsible for ensuring:**
    - **The device has a good standard of up-to-date anti-virus and security software installed**
    - **Be protected by a password, PIN, or biometric security.**
    - **If the personal device has been lost, hacked or security compromised, the Clerk is to be informed, and the necessary steps taken.**
    - **The personal devices of councillors and staff are considered 'authorised' so long as appropriate steps have been taken to secure them.**
- **When a councillor or member of staff leaves the Council, they must delete all Council emails and data from their personal devices.**

6. Leavers and Account Management

- **When a councillor or member of staff leaves the Council:**
    - **Their Council email account password will be changed**
    - **The account will be closed and deleted in line with retention requirements**
    - **Access to all Council ICT systems will be removed**

7. Anti-Virus and System Security

- **All Council-owned computers and devices must:**
    - **Have approved anti-virus software installed**
    - **Be scanned for viruses and malware at least once per month**

- **Receive regular software and security updates where possible**

8. Email and Internet Security

- **Users must not click on links or open attachments in emails they do not trust or recognise.**
- **Suspicious emails must be:**
  - **Flagged as suspicious or phishing**
  - **Reported immediately to the Clerk**
  - **The Clerk is to inform the other councillors to access the situation**
  - **The flagged email is to be permanently deleted for the account**
  - **A virus scan on the device is to be conducted**
  - **If needed the passwords for the account will be changed via the Clerk**
- **Users must remain vigilant to cyber threats, including phishing, spoofed emails, and fake invoices.**

9. Data Breaches and Security Incidents

- **Any suspected or actual data breach, cyber incident, or loss of information must be reported immediately to the Clerk.**
- **The Clerk will assess the incident in line with the Council's Data Protection Policy and UK GDPR requirements.**
- **Where required, the data breach will be reported to the Information Commissioner's Office (ICO) within the statutory timeframe.**
- **Following a data breach:**
  - **Relevant account passwords will be changed immediately**
  - **Affected accounts and devices will be scanned using approved anti-virus software**
  - **Any compromised access will be suspended**
  - **Lessons learned will be recorded to reduce the risk of recurrence**

This section must be read in conjunction with the Council's Data Protection Policy, Privacy Notices, and Records Retention Policy.

10. Cyber Fraud, Phishing, and Invoice Scam Prevention

Cyber-enabled fraud presents a significant risk to local councils. Tiptree Parish Council adopts a zero-tolerance approach to cyber fraud.

- **Staff and councillors must remain vigilant to:**
    - **Fake or altered invoices**
    - **Requests to change bank details**
    - **Emails purporting to come from councillors, staff, contractors, or suppliers requesting urgent payments**
- **Bank detail changes must always be verified using an independent method (e.g. known telephone number).**
- **Payment instructions must never be accepted or actioned solely by email.**
- **Any suspected fraud or scam must be reported immediately to the Clerk and RFO.**

11. Responsibilities

Full Council

- **Has overall responsibility for ensuring that appropriate ICT and information security arrangements are in place.**
- **Adopts and reviews this policy.**

Clerk to the Council (Proper Officer)

- **Has day-to-day responsibility for ICT security and data protection compliance.**
- **Acts as the primary point of contact for data breaches, cyber incidents, and suspected security risks.**
- **Ensures that Council email accounts and access rights are managed appropriately.**
- **Liaises with external IT providers, the ICO, and other relevant bodies as required.**

Responsible Financial Officer (RFO)

- **Ensures that financial systems and data are protected in line with this policy.**
- **Works with the Clerk to reduce the risk of fraud, cyber-enabled financial crime, and unauthorised access to financial information.**

Councillors, Staff, Contractors, and Volunteers

- **Must comply fully with this policy and any related procedures.**

- **Are responsible for safeguarding Council equipment, accounts, and information allocated to them.**

- **Must report any suspected or actual security incidents without delay.**

12. Breach of Policy

Failure to comply with this policy may result in:

- **Removal of access to Council systems**

- **Disciplinary action (for staff)**

- **Referral to Council or relevant authorities where appropriate**

13. Review of Policy

This policy will be reviewed by the Council at least every two years, or sooner if required due to legislative changes, audit recommendations, or operational need.

14. Acceptable Use Declaration

All councillors, staff, contractors, and volunteers who access Council ICT systems or data must confirm their understanding of and agreement to this policy.

Declaration

This declaration applies to all councillors, staff, contractors, and volunteers.

I confirm that I have read, understood, and agree to comply with the Tiptree Parish Council IT & ICT Security Policy. I understand that failure to comply may result in access being withdrawn and/or disciplinary or other appropriate action being taken.

Name: _____

Role (Councillor / Staff / Contractor / Volunteer): _____

Signature: _____

Date: _____

Appendix A – Quick Guide for Councillors and Staff (Dos and Don'ts)

This quick guide applies equally to councillors and staff and should be read alongside the full IT & ICT Security Policy.

Do:

- **Use your Council-provided gov.uk email account for all official Council business.**
- **Keep passwords secure and do not share them with anyone.**
- **Check emails carefully for signs of phishing or fraud.**
- **Report suspicious emails, links, or attachments to the Clerk immediately.**
- **Ensure any personal device used for Council business has up-to-date anti-virus software.**
- **Lock your screen and log out when leaving a device unattended.**
- **Report any loss of devices, data, or suspected breaches immediately.**

Do Not:

- **Use personal email accounts for Council business.**
- **Click on links or open attachments from unknown or unexpected senders.**
- **Share Council information with unauthorised individuals.**
- **Store Council data on unapproved cloud services or personal storage devices.**
- **Reuse Council passwords on other websites or services.**

Appendix B – Website Publication Statement

To support transparency and awareness, Tiptree Parish Council will publish a short summary of its IT & ICT Security arrangements on the Council website.

The website section will:

- **Confirm that the Council uses secure gov.uk email accounts for councillors and staff**
- **Explain that personal email accounts are not used for official Council business**
- **Confirm that the Council takes cyber security, data protection, and GDPR compliance seriously**
- **Provide contact details for reporting suspected data protection or security concerns**

No sensitive security information or technical system details will be published on the website.