TOLLESHUNT KNIGHTS PARISH COUNCIL

IT POLICY
Adopted at the meeting dated 15.6.2026
Review date June 2027

1. Introduction

Tolleshunt Knights (the Council) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all users of IT resources, including computers, networks, software, devices, data, and email accounts. The Council endeavours to provide digital devices but acknowledges that some small Council staff and members may be using their own personal devices. All users must adhere to this policy to maintain digital security.

3. Training and awareness

The Council will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. Individuals (Councillors and employees) should engage in regular training on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service's virtual cybersecurity workshops for councils

- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. Acceptable use of council provided IT resources and email

When using IT resources for the Council's purposes, users must adhere to ethical standards, and respect copyright and intellectual property rights.

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks.

Users must not install unauthorised software without checking with the clerk, and must not use equipment or email to access or forward inappropriate or offensive content.

5. What Users must do if they use their own personal devices

The Council will endeavour to provide users with devices to use for council business. If users are using their own device they must make sure they are:

- using strong passwords for all accounts (preferably using a password manager)
- downloading the latest operating system security updates
- using anti-virus software

Where users work remotely or use personal devices:

- Devices should be password protected
- Screens should not be left unattended
- Confidential information must be secured
- Public or shared computers should be avoided
- Council data should not be stored permanently on personal devices unless authorised

The Council may require security measures on devices used for Council business.

6. Network and internet usage

Users must not:

- Access inappropriate or illegal content
- Download copyrighted material unlawfully
- Introduce malicious software
- Access unsecured Wi-Fi for sensitive work without appropriate safeguards

7. Password and account security

Users are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

8. Email communication

The Council will endeavour to provide users with an official email account for organisation-related communication only. If users are currently using a personal email account, they should aim to move over to an official email account as soon as practically possible. Users must make sure that emails are professional and respectful in tone. Users must always check they are sending any confidential or sensitive information to the correct recipients.

Users are required to be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

9. Email access

The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they respond to FOI or subject-access requests. The use of personal email accounts for council business is prohibited.

10. Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. Users must regularly backup any important data to prevent data loss and follow the Council's data retention policies.

Users should retain and archive emails in compliance with the Council's data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

11. Software and Licensing

Only authorised software may be installed on Council devices.

Users must not:

- Install unlicensed software
- Download unauthorised applications
- Modify system settings without permission

The Council will maintain appropriate software licences where required.

12. Data Storage and Backups

Council information should be stored in approved locations such as:

- Approved cloud services
- Official Council storage systems

Important records must be backed up regularly.

Users must avoid storing Council data solely on:

- USB drives
- Personal cloud accounts
- Unsecured personal devices

13. Social Media and Website Management

Only authorised persons may:

- Publish content on behalf of the Council
- Access Council social media accounts
- Update the Council website

Official communications must:

- Be accurate and professional
- Comply with legal obligations
- Avoid political bias

Passwords for Council accounts must be retained securely and accessible to the Clerk and appropriate officers.

14. Reporting security incidents

Users must immediately report:

- Lost or stolen devices
- Suspected malware infections
- Unauthorised access
- Phishing attempts
- Data breaches
- System vulnerabilities

All suspected security breaches, including email breaches or incidents should be reported immediately to the Parish clerk.

15. Compliance and consequences

Breach of this IT and Email Policy may result in:

- Withdrawal of IT access
- Disciplinary action
- Referral to law enforcement where appropriate

Serious breaches may constitute gross misconduct.

16. Business Continuity

The Council will take reasonable steps to maintain continuity of critical systems and information, including:

- Regular backups
- Password recovery arrangements
- Retention of administrative access details
- Contingency arrangements for key systems

17. Staff or Councillors leaving the council – exit procedure

- Account passwords will be changed by the Clerk or authorised person, including email, cloud storage, accounting package, etc.

- Any council-owned equipment will be returned to the clerk within one week.
- An email will be sent to the Clerk confirming that all Council data has been removed from personal devices

18. Policy review

This policy will be reviewed annually or sooner if:

- Legislation changes
- Technology changes significantly
- Security incidents indicate revision is necessary

19. Contacts

For IT-related enquiries or assistance, users can contact the Parish clerk.

All staff and councillors are responsible for the safety and security of IT and email systems.

Date of adoption: The above policy was adopted at the Parish Council's meeting dated ******** and recorded as Minute reference *******

Date for next review: June 2027