

TINTINHULL PARISH COUNCIL IT POLICY

1. Introduction

Tintinhull Parish 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. Alongside the appropriate use of other information, usually delivered on paper media, created by or delivered via the Council.

2. Scope

This policy applies to all individuals who use Tintinhull Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. Further, it applies to all Councillors and officers who access Council email or documents using a personal device.

3. Acceptable use of IT resources and email

Tintinhull Parish Council IT resources and email accounts are to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

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

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

Staff and Councillors should not be allowed to access information until the Clerk is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

All sensitive and confidential Tintinhull Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

All devices must:

- Be secured with a strong password/PIN/Biometrics and auto-lock after inactivity.

- Use encryption where available.

- Be kept updated with latest operating system and security patches.

Council data must be accessed only through approved applications

Use of removable media (USBs, SD cards) for Council data is prohibited unless encrypted.

6. Disclosure of Information - Computer and Paper Based

The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a User treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is to be reported to the delegated Data Controller (Clerk) who will take appropriate action.

Disposal methods for waste computer-printed output and other media must be in accordance with Tintinhull Parish Council's Document Retention and Disposal policy.

Distribution of information should be via the most secure method available.

Users should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

7. Network and internet usage

Tintinhull Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

8. Telephone communication

Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.

For external callers, verify their identity and their need to know the requested information.

Telephone them back before releasing information and ask the caller to provide evidence of their identity.

- Ensure that you are authorised to disclose the information requested.
- Ensure that the person is entitled to be given this information.
- Ensure that the information you give is accurate and factual.

9. Email communication

- Email accounts provided by Tintinhull Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.
- Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.
- Personal or sensitive information is at risk if sent outside of the Council's network.
- If an email is sent to an address that is not a Council domain address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted.
- Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure.
- The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.
- No identifiable personal information should be included when sending on emails.
- The recipients of Tintinhull Parish Council emails are prohibited from being forwarded, copied or blind copied to any third party within or outside of the Council.
- Any Councillor email contact with a member of the public shall be directed to the Council Office for the attention of the delegated Data Controller (Clerk).

10. Password and account security

Tintinhull Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

11. Mobile devices and remote work

Mobile devices should be secured with passcodes and/or biometric authentication.

When working remotely, users should follow the same security practices as if they were in the office. Personal and council data must be kept separate (e.g. using distinct apps).

Councillors must only use council data for council business.

Council data must not be backed up to personal cloud accounts, public data and backup services (e.g. Dropbox, Google Drive) or shared with third-party apps.

Users must not use publicly available wi-fi networks (e.g. in airports, hotels, cafes, restaurants and libraries) to access council data.

Users must not circumvent Council controls, download and/or copy council data to or from their personal devices.

Users must not screenshot, screengrab or take photos of Council data on their personal devices.

Users must not allow their family members, friends or other individuals access to any device that is logged into the Council system and any data and systems accessed through it.

Users must be aware of their surroundings when accessing Council data.

Any personal device used may be subject to 'discovery in litigation'. This means that it could be used as evidence in a lawsuit against the Council. Your data could be examined by representatives of the Council and also by other parties in any lawsuit.

Devices must allow for remote wipe or manual deletion of Council data.

12. Email monitoring

Tintinhull Parish Council reserves the right to monitor email communications to ensure compliance with this policy and applicable laws. Monitoring will be carried out in accordance with the Data Protection Act and GDPR.

13. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

14. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Parish Clerk

15. Training and awareness

Tintinhull Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All staff and Councillors will receive training on email security and best practices.

16. Compliance and consequences

Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

The Council may require confirmation that devices meet these security standards. No monitoring of personal use will be carried out beyond ensuring Council data is protected.

Councillors remain personally responsible for protecting Council data on their device. On leaving office, Councillors must ensure all Council data is securely deleted and access revoked.

17. Policy review

This policy will be reviewed every three years (or sooner should applicable legislation change) to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

18. Contacts

For IT-related enquiries or assistance, users can contact parish clerk parishclerk@tintinhull.online

All staff and Councillors are responsible for the safety and security of Tintinhull Parish Council's IT and email systems. By adhering to this IT Policy, Tintinhull Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Policy agreed on