TUTBURY PARISH COUNCIL IT POLICY

1. Purpose

This policy outlines the principles and procedures for the use, management, and security of IT systems, devices, and data within Tutbury Parish Council. It aims to ensure that technology is used responsibly, securely, and in compliance with legal and regulatory requirements.

2. Scope

This policy applies to:

- All Parish Council members and employees
- All devices, software, and digital services used for Council business

3. IT Governance

- The Clerk is responsible for day-to-day IT management and liaising with external IT providers.
- The Council will ensure appropriate budget provision for IT maintenance, upgrades, and cybersecurity.
- All IT purchases must be approved by the Council and comply with procurement procedures.
- If an item of portable equipment is lost or damaged this should be reported to the council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first 50% of the loss/damage.

4. Use of own devices

- The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, including, but not limited to, reading their emails, accessing documents stored on the council's one drive or to store data. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.
- However, the same security precautions apply to personal devices as to the council's desktop equipment. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.
- Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.
- If you use your personal device to access council information, you are responsible for protecting the device. This includes ensuring the device is not used by anyone else to gain access to council information – even if you think the information is not confidential.
- Breach of this, or any other Parish Council policy may result in disciplinary ac on or, in case of councillors, a referral to the Monitoring Officer.

5. Acceptable Use

- Council IT systems and devices must be used only for official Council business.
- Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk. Any personal use of our computers and systems should not interrupt our daily council work in any way.
- Users must not install unauthorised software or access inappropriate content.
- All communications via Council email or social media must be professional and in line with Council values.

6. Data Protection and Privacy

- All personal data must be handled in accordance with the UK GDPR and Data Protection Act 2018.
- The Clerk is the designated Data Protection Officer (DPO) and responsible for ensuring compliance.
- Personal data must be stored securely and only accessed by authorised personnel.
- Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements,
- Data breaches must be reported immediately to the Clerk and documented.

7.0 Password and Authentication Policy

- All user accounts must be protected by strong, secure passwords
- In addition to strong passwords, Multi-Factor Authentication (MFA).
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chair of the council, in a sealed envelope, only to be accessed in an emergency.
- (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

8. Email and Communication

- Council members and Clerk email accounts must be used for all official correspondence.
- Emails must be archived and retained in accordance with the Council's Document Retention Policy.
- All councillors, staff, and other authorised users who need to use email as part of their role will normally be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.
- Clerk emails to Councillors are intended only for the named recipient and may be privileged or confidential, members are reminded not to copy or distribute outside of Council.
- Clerk will have the following in the email signature: The information in this email is intended only for the named recipient and may be privileged or confidential. If you are not the intended recipient, please notify the Clerk immediately and then delete the message and do not copy, distribute or take action based on this email.

9. Website and Social Media

- The Clerk is responsible for maintaining the Council website and social media, and ensuring content is accurate and up to date.
- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.

- The council will abide by the Parish council's Social Media policy.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.

10. Security and Access Control

- Devices must be password-protected , encrypted and updated regularly.
- Access to sensitive data and systems must be restricted to authorised users.
- Remote access must be secured via VPN or encrypted connections.
- Anti-virus and firewall protection must be maintained on all Council devices.

11. Backups and Disaster Recovery

- Regular backups of Council data must be performed and stored securely.
- A disaster recovery plan must be maintained to ensure continuity of operations in the event of IT failure or data loss.

12. Reporting and Enforcement

- Any IT issues, security concerns, or suspected breaches must be reported to the Clerk immediately.

13. Copyright

- Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.
- It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.
- Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).
- Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

- Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the clerk" if unsure about anything.

14. Use of Artificial Intelligence (AI)

- Artificial intelligence tools may be used to assist in drafting documents or generating content. Any material produced using AI must be reviewed by a councillor or officer before use to ensure accuracy and compliance with copyright law. Councillors, staff and authorised users must not upload copyrighted, confidential or personal data into AI systems without appropriate permission or authority.

15. Accuracy of information

- One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

16. Review and Updates

- This policy will be reviewed if required due to changes in legislation, technology, or Council operations.

17. Other Policies to read with this policy
Media Policy, Retention and Disposal of Documents, Business Risk Analysis, Freedom of Information and Publication Scheme, Data Protection Policy, Social Media Policy.

This policy has been adapted from guidelines issued By NALC .

Date last Ratified/Approved	Version Number	Revision/Amendment Made	New Review date
March 2026	1	Policy adopted	March 2027