TOSTOCK PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) POLICY

Adopted 2026-03-10

---

1 Introduction

1.1 This IT Policy establishes clear parameters for how councillors and the Clerk use technology or equipment in the course of their duties and applies regardless of where any work is being carried out. It is intended to:

- set expectations for appropriate use of equipment and systems;
- raise awareness of risks associated with IT use;
- safeguard Council data and digital assets;
- clarify what constitutes acceptable and unacceptable use; and
- outline the consequences of policy breaches.

1.2 Tostock Parish Council recognises the importance of effective and secure information technology, including e-mail usage, in supporting its business, operations and communications.

1.3 By adhering to this policy the Council aims to create a secure, efficient and effective IT environment that underpins and facilitates its work, mission and goals.

2 Scope

2.1 This policy applies to councillors and the Clerk (and any authorised others) who use IT resources on behalf of the Council - computers, networks, software, data, websites and e-mail - regardless of whether they are Council owned/provided, or personal devices.

2.2 The Clerk is responsible for day-to-day IT management and liaising with any IT providers used by the Council. The Council will provide for and ensure appropriate budget provision for IT procurement, maintenance, upgrades and cybersecurity.

3 Acceptable Use of IT Resources and E-Mail

3.1 Any and all Council IT resources and e-mail accounts are to be used for official Council-related activities and tasks only. Personal use is not permitted.

3.2 Users must adhere to ethical standards, respect copyright and intellectual property rights and avoid accessing inappropriate or offensive content.

3.3 Councillors are encouraged not to use personal e-mail accounts for Council business.

4 Device and Software Usage

4.1 As and when appropriate, authorised devices, software and applications will be provided by the Council for work-related tasks. This will apply principally in the case of the Clerk who may be supplied with a PC or laptop, relevant software and

printer. In such circumstances, any device(s) must be returned when the post-holder leaves the role.

4.2 Computer and any other electronic equipment supplied should be treated with good care at all times. Such equipment is expensive, and any damage sustained will have a financial impact on the Council.

4.3 The unauthorised installation of software on any Council-provided device is strictly prohibited due to security concerns. Likewise, personal disks, USB sticks and similar data storage devices etc. cannot be used on Council computers.

4.4 The Council recognises that some councillors and the Clerk may wish to use their own smartphones, tablets, laptops etc. for normal Council purposes, e.g. accessing e-mails and documents. The same security precautions apply to personal devices as to any Council desktop equipment.

4.5 The Clerk and councillors that use Council systems are expected to use any and all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device paid for or provided by the Council carries a high degree of risk. For the Clerk this may result in disciplinary action, including summary dismissal (without notice).

4.6 In the (unlikely) case of any legal proceedings against the Council it may need to temporarily take possession of a device, whether Council-owned or personal, to retrieve relevant data encompassed by the situation.

4.7 Councillors and the Clerk must maintain a clear separation between personal data processed on behalf of the Council and that processed for his/her own personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

4.8 Councillors and the Clerk who intend to use their own devices must ensure that they:

- use a strong password to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after three failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than three minutes;
- always password protect any documents containing confidential information that are sent as attachments to an e-mail, and notify the password separately (preferably by a means other than e-mail);
- for smartphones and tablets, activate the automatic device wipe function (where available);
- ensure secure Wi-Fi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device; and

- inform the Clerk (or Chair) if his/her device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to Council data or resources.

4.9 Personal data relating to councillors, the Clerk, associates, residents and external stakeholders and others should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen.

4.10 Personal information and sensitive data should never be saved on personal devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

4.11 If removable media, e.g. USB drives, are used to transfer data the user must also securely delete the data on the media once the transfer is complete.

4.12 Councillors and the Clerk who open any attachments should ensure that any cached copies are deleted immediately after use. Additional risks include data belonging to the Council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the permission of the owner.

4.13 Any Council work done on a user's own equipment must not only be stored separately, but also securely. Further, it should be password protected and always be backed up.

4.14 Prior to the disposal of any device that has work data stored on it, and in circumstances when any councillor and/or the Clerk leaves the Council, appropriate action must be taken to ensure that all passwords and any identifiable data are securely removed.

5 Health and Safety

5.1 The Council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to the Clerk to provide for the proper and safe use of display screen equipment.

5.2 Should the Clerk feel that his/her workstation requires changes to make it compliant then he/she must speak to the Chair. If any hazards are detected at a workstation, this should likewise be reported immediately to the Chair so that appropriate remedial action can be discussed and effected.

6 Monitoring of IT Use

6.1 The Council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors and the Clerk

are properly informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

6.2 The Council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, computers, or associated technology to ensure compliance with this policy as well as relevant legislation.

6.3 Information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

6.4 Councillors and the Clerk have a number of rights in relation to their personal data, including the right to make a subject access request and the right to have data rectified or, in some circumstances, erased.

6.5 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether IT use is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

7 Remote Working

Increased IT security measures apply to councillors and the Clerk who work from home, as follows:

- if logging into any Council system remotely, using computers that either do not belong to the Council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people;
- any data printed should be collected and then stored securely;
- all electronic files should be password protected and the data saved to the Council IT facility when accessible;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drives or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the vehicle.

8 Data Management, Retention and Security

8.1 All sensitive and confidential Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed (quarterly as a minimum) to, as far as reasonably possible, prevent data loss and secure data destruction methods should be used when necessary.

8.2 The Council is committed to the role of Data Controller and thereby the protection of personal data in relation to and to be compliant with the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), and any and all other data protection legislation applying in the UK.

8.3 The Clerk is the designated Data Protection Officer for the authority.

8.4 No personal data relevant to the Council should be stored unencrypted on any personal devices or iCloud platforms.

8.5 Full information about how the Council processes personal data can be found in its Data Protection Policy.

8.6 How the Council handles and provides access to recorded information is set out in its Freedom of Information Policy and related Publication Scheme.

8.7 The Council recognises that the efficient management of its data and records is essential to comply with its legal and regulatory obligations, and to contribute to the effective management and governance of the Council. Data retention (including that of e-mails) will, therefore, be managed effectively to be consistent with prevailing legislation as set out in its Data and Records Retention Policy.

8.8 For residents and the public generally, how it processes personal data is set out in its Privacy Notice as published on its pages on the village website.

9 Website

9.1 The Council actively supports the principle of openness, transparency and accountability and will continue to improve access to information, not least on a proactive basis through its pages on the village website.

9.2 The Council is fully compliant with the publication requirements of the *Transparency Code for Smaller Authorities* (published by the Department for Communities and Local Government, December 2014).

9.3 Parish Council pages on the village website are managed by the Clerk.

9.4 The Public Sector Bodies Accessibility Regulations 2018, which came into force on 23 September 2018, seek to ensure that public sector websites are accessible to all users, especially those with disabilities. Should there be any barriers then a statement will inform users of alternative routes to access as well as enabling users to contact the website owner if they identify issues. Through its website provider the Council is fully compliant, in terms of accessibility, with WCAG 2.2 AA standards (an internationally recognised set of recommendations for improving web accessibility which authorities are required to be achieved by the Government).

10 Social Media

10.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user-generated media sites; social networking sites (e.g. Facebook, X, TikTok, etc.); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at all times.

10.2 The Council acknowledges that councillors may wish to join in with and help to shape sector conversation, and enhancing its image through blogging and interaction in social media.

10.3 It must be remembered that inappropriate comments and postings can reflect negatively upon the Council. To protect both the Council and its interests, councillors and the Clerk are required to comply with the following, whether in relation to their Council role or personal social networking sites:

- even if the Council is not mentioned specifically, care should be taken with views expressed on social media sites and any postings should clearly be stated to be the writer's own;
- councillors and the Clerk are expected to be respectful about the Council and not to engage in any behaviour that will adversely affect its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is unacceptable and could constitute gross misconduct.
- comments posted by councillors and the Clerk on any sites should not compromise the Council in any way;
- any writing about or displaying photos or videos of internal activities that involves current councillors and/or the Clerk might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the Council should not be posted;
- councillors and the Clerk must be aware that they are personally liable for anything that they write online. Councillors should always be mindful of the Model Councillor Code of Conduct 2020. The Clerk may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, proprietary, harassing, libellous, or that might create a hostile work environment;
- postings to websites or anywhere on the Internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the Council or disclose personal data or information about any individual that could breach data protection legislation;
- contacts by the media relating to the Council, should be referred to the Clerk or Chair; and

- councillors and the Clerk who may leave the Council must not post any inappropriate comments about the Council, councillors or the Clerk on any social media/networking sites.

10.4 It is important to note that contact details and information remain the property of the Council. In addition, councillors and the Clerk upon leaving the Council will be required to delete all Council-related data held (including contact details) from any personal device/equipment.

11 E-Mail Communication

11.1 The official Council e-mail account (clerk@tostock-pc.gov.uk) is primarily for use by the Clerk for all formal communications. In circumstances where he/she is absent then the Chair may access the same address to receive and/or issue communications on behalf of the Council.

11.2 Wherever possible, councillors will be given their own Council e-mail address and account to provide for their formal role.

11.3 All e-mails should be professional and respectful in tone.

11.4 Personal use of the Council e-mail account is not permitted.

11.5 Confidential or sensitive information must not be sent via e-mail unless it is encrypted.

11.6 Care should be exercised when opening e-mails with attachments and/or links to avoid phishing and malware. E-mail sources should be verified whenever and wherever possible.

11.7 The forwarding of Council e-mail to private addresses is prohibited.

11.8 The Council reserves the right to monitor e-mail communications to ensure compliance with this policy and relevant laws. Any monitoring will be conducted in accordance with prevailing data protection legislation.

11.9 Access to the Council e-mail account should be via an appropriately strong password which is shared only between the Clerk and Chair, with others included should exceptional circumstances apply.

12 Internet Use and Copyright

12.1 Any Council network and Internet connections should be used responsibly, effectively and efficiently for official business purposes only. Downloading and sharing copyrighted material without proper authorisation is prohibited.

12.2 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). 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, damages being awarded and disciplinary action, including dismissal, being taken against the perpetrator.

12.3 Council policy is to comply with copyright laws. Neither councillors nor the Clerk should 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 but is still copyright protected) and information which is not protected by copyright. A website will usually contain copyright conditions and such warnings should be read before downloading or copying.

13 Password and Account Security

13.1 Councillors who choose to use personal e-mail accounts for Council communications are responsible the security of their accounts and passwords.

13.2 Council passwords should be strong - a minimum of 10 characters (upper and lower case letters, numbers and symbols) - not shared with any others or personal facilities under any circumstances, and changed regularly (at least every six months) to encourage, ensure and enhance security.

13.3 Passwords must not be stored in plain text or written down in insecure locations.

13.4 Any password which has been identified as being compromised, or is suspected to have been compromised, should be changed immediately.

14 Mobile Device

Any mobile device which may be provided/issued to the Clerk should be secured with an appropriate passcode and/or biometric authentication.

15 Meetings

15.1 Except where members of the public are excluded due to the confidential nature of the business being considered, any person may film, photograph, audio record or use social media to report on Council meetings. Any person intending to report in this way will be expected to notify the Clerk or Chair before the start of the meeting.

15.2 Under no circumstances should any non-public meeting, conversation or similar be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

16 Security Incidents

16.1 Any IT device used for the storage or transmission of Council data must be equipped with current anti-virus protection.

16.2 A suspected security incident should be reported, as soon as it is discovered, to the Clerk and/or Chair of the Council and, if appropriate, the website and e-mail provider.

16.3 Action should be taken immediately to safeguard the situation and to apply a remedy to the position should this be achievable.

17 Training and Awareness

The Council will provide and/or make available regular training and resources to educate councillors and the Clerk about IT, security, best practices and privacy concerns. Relevant technology updates will also be delivered when available.

18 Compliance and Consequences

Any breach of this policy will be viewed seriously by the Council. In the case of the Clerk, disciplinary action may be taken. Where a breach is found to be due to a councillor then any consequence will be subject to the nature of the breach and the action permitted to be taken in the circumstance.

19 Policy Review

This policy will be reviewed annually by the Clerk to ensure it is up-to-date, relevant and effective, and changes reported to the Council. Updates will be made to provide for new and/or changing legislation, and to address emerging technology trends and security measures.