TOLLER PORCORUM PARISH COUNCIL

DRAFT Information Technology (IT) Policy

Adopted: 14 January 2026 | Next review date: May 2027 | Last review date: 14 January 2026

Contents

Purpose

The purpose of this IT policy is to establish clear parameters for how councillors, employees and other authorised users use council-provided technology or equipment in the course of their duties. It also sets clear parameters for how councillors use their own devices in the course of their duties. This policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

Monitoring of IT use

As an IT provider, 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, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g.: if they have a council e-mail address.

TOLLER PORCORUM PARISH COUNCIL

COMPUTER USE

1. Hardware

1.1 Council computer equipment is provided for council purposes only.

1.2 All councillors, employees and other authorised users must lock their computers when they are left unattended to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

1.4 Computer and electronic hardware should be kept clean and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.5 A database of equipment issued will be kept.

1.6 Equipment should not be dismantled or reassembled without seeking advice.

1.7 Councillors, employees and other authorised users are not to purchase any computer or mobile equipment (including software) unless previously authorised.

1.8 Personal disks, USB stick, CDs, DVDs and data storage devices etc cannot be used on council computers without the prior approval of the council.

1.9 Any faults or necessary repairs must be reported to the council.

EQUIPMENT

2. Portable equipment

2.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.2 It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

2.3 All portable computers must be stored safely and securely when not in use, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

2.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All laptops, smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

2.5 If an item of portable equipment is lost or damaged this should be reported to the clerk or the chair of the council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the first [specify amount] of the loss/damage.

2.6 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises,

without the prior written permission of the council. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

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

2.8 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from clerk.

HEALTH AND SAFETY

3. Councillors, employees, and other authorised users who work in council offices will be provided with an appropriate workstation.

3.1 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment (DSE). Further details are set out in the council's Homeworking Policy.

3.2 Any DSE user who feels that their workstation requires changes to make it compliant must speak to the Staffing Committee.

3.3 If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Staffing Committee.

PASSWORDS AND AUTHENTICATION

3. All user accounts of council owned services must be protected by strong, secure passwords.

3.1 The council aims to follow the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

3.2 In addition to strong passwords, Multi-Factor Authentication (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.

3.3 To further strengthen account security:

a. Initial user account passwords must be generated by the clerk.
b. Default passwords provided by vendors or the clerk must be changed immediately upon installation or setup.
c. Service or System (e.g. Website) account passwords are generated and managed by the clerk.

d. The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

3.4 Access to Passwords

a. Passwords are personal and must not be shared under any circumstances.
b. Only the assigned user of an account may access or use the associated password.
c. In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to the chair of council with appropriate approvals and logging.
d. Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chair of council], in a sealed envelope, only to be accessed in an emergency.

3.5 Password Storage and Management

a. Passwords must not be stored in plain text or written down in insecure locations.
b. Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

3.6 Password Change Requirements

a. Immediately change password if compromise is suspected.

3.7 Password Access Control and Logging

a. All access to administrative or shared credentials must be logged and auditable.
b. Attempts to access unauthorized passwords will be treated as a security incident.

3.8 Responsibility

a. Users are responsible for creating and maintaining secure passwords for their accounts.
b. The clerk, as IT security provider, is responsible for:
    i. Managing system/service credentials.
    ii. Enforcing password policies. Auditing and monitoring password-related security practices.

BACKUP PROCEDURES

4. The council's digital files and documents are stored in a secured Microsoft One Drive cloud storage and on a solid hard drive.

4.1 The council's Microsoft One Drive cloud storage is password protected and is accessed by the council's laptop, provided to the clerk.

4.2 At the end of each financial year, all files and documents are copied to the council's solid hard drive which is deposited with the chair of council for safe keeping.

MONITORING

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

5.1 Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

5.2 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

5.3 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.4 The information obtained through monitoring may be shared internally, including with relevant councillors and employees if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

5.5 The 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.

5.6 Councillors, employees, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

5.7 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system 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.

5.8 The council will ask for access to the council's laptop from time to time to monitor all internet usage. The council will view internet activity, which details the names of all websites accessed, along with the date and time of access, by employees and other authorised users. Records of internet use and sites visited will normally be retained for a period of six months but the council understands that browsing history may need to be deleted within this timeframe to optimise performance of the laptop when accessing necessary websites.

5.9 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

5.10 Any use that the council considers to be “improper”, either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.11 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

REMOTE WORKING

6. The council does not have premises and employees working from home are considered to be working at their normal place of work.

6.1 Remote working includes, but is not limited to, working whilst travelling, from other premises or any other different venue, and increased IT security measures apply in these circumstances as follows:

a. if logging into the council’s systems or services 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. If the configuration of the devise does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
b. 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, including other travellers on public transport etc;
c. any data printed should be collected and stored securely;
d. all electronic files should be password protected and the data saved to the council’s system/services when accessible;
e. papers, files or computer equipment must not be left unattended at a non council premises unless arrangements have been made with a responsible person at non council premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time;
f. any data should be kept safely and should only be disposed of securely;
g. papers, files, data sticks/storage, flash drive 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 car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
h. where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;
i. Councillors, employees, and other authorised users who work away from their normal place of work with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

6.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

6.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

EMAIL

7. Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, employees, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

7.1 Email is the council's primary means of communication. On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Councillors, employees, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

7.2 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, employees, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, employees, and other authorised users should ask the clerk, rather than assuming they know the right answer.

7.3 All councillors, employees, 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.

7.4 Email messages sent on the council's account are for council use only. Personal use is not permitted.

7.5 Use of email will comply with the council's Digital Communication and Social Media Policy.

USE OF THE INTERNET

8. Copyright

8.1 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.

8.2 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.

8.3 Councillors, employees, 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).

8.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

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

9. Trademarks, links and data protection

9.1 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.

9.2 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.

9.3 Councillors, employees, 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).

9.4 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

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

10. Accuracy of information

10.1 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.

USE OF SOCIAL MEDIA

11. Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites like YouTube; social networking sites such as Facebook, LinkedIn, X, Instagram, TikTok, etc.; virtual worlds like Second Life; 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 any time, either using council systems or at home.

11.1 Personal use of social networking/media and chat sites are not permitted on council owned devices.

11.2 The council recognises the importance of councillors, employees, and other authorised users joining in and helping to shape sector conversation and enhancing its image through

blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

11.3 However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks about those the council does business with could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, employees, and other authorised users should be aware that parishioners or other local organisations may read councillors, employees, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

11.4 To protect both the council and its interests, everyone is required to comply with the council's Digital Communication and Social Media Policy in relation to social media and their council role or personal social networking sites, irrespective of whether this is during or after working hours.

11.5 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, employees, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

11.6 It is important to note that contact details and information of those the council does business with, remain the property of the council. In addition, councillors, employees, and other authorised users leaving the council will be required to delete all council-related data including contact details of those the council does business with from any personal device/equipment.

MISUSE

12. Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

USE OF OWN DEVICES

13. Councillors and other authorised users may use their own smartphones, tablets, laptops etc to conduct council business.

13.1 Such devices can be used to access council servers, storage clouds or networks for normal council purposes, including, but not limited to, reading emails, accessing council documents (should permission be granted by the clerk) or to access data in other services.

13.2 Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. 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.

13.3 However, the same security precautions apply to personal devices as to the council owned 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.

13.4 Councillors and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk. For Workers or Contractors, the council may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

13.5 In cases of legal proceedings against the council or external stakeholders, the council may need temporary access to or to temporarily take possession of a device, whether council-owned or personal, to retrieve the relevant data.

13.6 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 council-related purposes.

13.7 Personal data relating to, but not limited to, councillors, employees, and other authorised users, associates, residents and external stakeholders should only be saved to personal accounts with third-party storage cloud service providers that are password protected and secure. To do otherwise may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if passwords used to store/access data are saved onto the device, or if the service permits councillors, employees, and other authorised users to remain logged in between sessions.

a. The same applies to personal information and sensitive data as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

b. Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

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

13.9 Councillors and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. The clerk will provide assistance or training in doing this if needed. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

13.10 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

13.11 Prior to the disposal of any device that has council data stored on it, and in the event of a user leaving the council, councillors and other authorised users are required to allow the clerk access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

13.12 Councillors and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

This policy is based on the model IT Policy provided by the National Association of Local Councils (NALC). It was commissioned in 2025 from Worknest HR, a company that provides HR advice and guidance to town and parish councils.