

IT and Electronic Communication Policy

Thurston Parish Council

Policy Approved: Policy & Resources Committee 20 August 2025 *revised March 2026*
Presented to Council: Full Council Meeting 1 April 2026
Review Body: Policy & Resources Committee
Review Period: Every two years or following legislative changes.
Next Review: Policy & Resources Committee November 2027

This document is subject to revision and is maintained electronically. Electronic copies are version controlled and printed copies are not subject to this control.

1. Introduction

The Parish Council understands that the use of digital and electronic communication enables it to interact in a manner that improves the communications both within the Parish Council and between the Parish Council and the people, businesses and agencies it works with and serves.

The Parish Council has a website and uses email to communicate. The Parish Council will always try to use the most effective channel for its communications. Should the Parish Council add to the channels of communication that it uses as it seeks to improve and expand the services it delivers, this policy will be updated to reflect the new arrangements.

2. Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined 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.

3. 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.

4. Communications form the Parish Council – Business Use

Communications from the Parish Council are expected to meet the following criteria:

- Be civil, tasteful and relevant;
- Not contain content that is knowingly unlawful, libelous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive;
- Not contain content knowingly copied from elsewhere, for which the Parish Council does not own the copyright;
- Not contain any personal information, other than necessary basic contact details;
- If official council business, it will be moderated by the Clerk to the Parish Council as the Proper Officer.

5. Monitoring

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. 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.

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.

Monitoring of a councillor's email 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.

The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff 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.

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.

6. Passwords

All user accounts must be protected by strong, secure passwords. The council follows 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.

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.

Passwords are personal and must not be shared under any circumstances.

Only the assigned user of an account may access or use the associated password.

In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.

If a compromise is suspected, the password should be reported to the Parish Clerk to enable a change to be actioned.

7. Parish Council website

Occasionally, the Parish Council may direct those contacting the Council to its website to see the required information if it is in the public domain. The website can be found at (https://thurstonparishcouncil.gov.uk/).

The Parish Council allows and enables approved local groups to have and maintain a presence on its website to present information about the group's activities. The local group will be responsible for maintaining the content and ensuring that it meets the Parish Council's 'rules and expectation' for the web site. The Parish Council reserves the

right to remove any or all of a local group's information from the web site if it feels that the content does not meet the Parish Council's 'rules and expectation' for its website. Where content on the web site is maintained by a local group it should be clearly marked that such content is not the direct responsibility of the Parish Council.

8. Parish Council email

Council email facilities are intended to promote effective and speedy communication on work-related matters. Councillors, staff, 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.

All councillors, staff, and other authorised users who need to use email as part of their role will be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that the system is being abused.

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

The Parish Council has a dedicated email address (info@thurstonparishcouncil.gov.uk). The email account is monitored and responded to during office hours and the Parish Council aims to reply to all questions sent as soon as practically possible.

The Clerk is responsible for dealing with email received and passing on any relevant mail to members or external agencies for information and/or action. All communications on behalf of the Council will usually come from the Clerk or Deputy Clerk and otherwise will always be copied to the Clerk. Financial matters will be received from the Responsible Financial Officer.

Please note that all office / administrative work part-time so will respond as soon as they can. The Parish Council may not respond to every comment it receives particularly if it is experiencing a heavy workload or the comment is for information purposes only.

Emails to the Parish Council become official and will be subject to The Freedom of Information Act. These procedures will ensure that a complete and proper record of all correspondence is kept.

The Clerk to the Council has their own email address: clerk@thurstonparishcouncil.gov.uk The Deputy Clerk can be contacted on admin@thurstonparishcouncil.gov.uk and the Responsible Financial Officer's on finance@thurstonparishcouncil.gov.uk .

9. SMS (texting)

Members and the Clerk may use SMS as a convenient way to communicate at times. All are reminded that this policy also applies to such messages.

10. Internal communication and access to information within the Parish Council

The Parish Council is continually looking at ways to improve its working and the use of electronic communications is a major factor in delivering improvement. Parish Councillors are expected to abide by the Code of Conduct in all their work on behalf of the Parish Council.

All Parish Councillors have a dedicated email given to them once elected or co-opted onto the Council and should ensure that they remove any council email addresses from their personal devices.

Council members should access their email via their MS365 log-in details. Members can easily bookmark this page to enable speedier access.

Schedule 12 to the Local Government Act 1972 covers meetings and proceedings of local authorities. Previously, paragraph 4(2)(b) requires principal and parish councils to send summonses to attend meetings by post to their members' home addresses, or under 4(4), by post, to an alternative address specified. In practice, this covered all the papers to be considered at meetings, not just the agenda.

The Government, under The Order made under Section 8 of the Electronic Communications Act 2000 amended Schedule 12 of the Local Government Act 1972 to allow local authorities to send their members summonses to attend meetings, including agendas and related papers to meetings, electronically.

The Parish Council has amended its own Standing Orders to allow the authorising of the use of electronic communication. Occasionally, the electronic communication may include attachments, such as a meeting agenda or papers, or a web-link enabling a parish councillor to view meeting papers.

As more and more information becomes available electronically, it is vital that all information is treated sensitively and securely. Parish Councillors are expected to maintain an awareness of the confidentiality of information that they have access to and not to share confidential information with anyone.

Failure to properly observe confidentiality may be seen as a breach of the Parish Council's Code of Conduct and will be dealt with through its prescribed procedures (at the extreme it may also involve a criminal investigation).

Members should be careful only to cc essential recipients on emails and avoid use of the 'Reply to All' option (whilst ensuring that the people who need to know the information are copied in) and ensure that email trails have been removed.

11. General Data Protection Awareness

Whilst parish councils are expected to comply with Data Protection legislation, individual Councillors will also need to ensure that they protect an individual's personal data whether it is stored electronically or as a hard copy. This applies only to living individuals (not the deceased, companies, other authorities and charities)

Personal data includes:

- Names and addresses
- Telephone numbers
- Email addresses
- IP addresses

Councillors are required to implement the following agreed measures to comply with the legislation:

- Only use Thurston Parish Council email account for parish council correspondence.

- Ensure all parish council correspondence includes the Thurston Parish Council footer containing the Privacy Statement or a link to the relevant page on the website (this will be provided by the Clerk).
- Ensure that all devices (computers, laptops, phones) are password protected.
- Not to forward on emails or email threads to a personal account as they may contain personal data.
- Delete emails which are no longer required.
- Where possible direct all correspondence to the Clerk who can obtain the necessary consent.
- Where possible avoid holding an individual's information in a Councillor's home or on a Councillor's own PC.
- If a Councillor has to hold any information containing personal data on behalf of the Parish Council, it needs to be stored securely in a locked room or cabinet or if on a PC, in an encrypted folder.
- Ensure that their antivirus software and operating system is up-to-date.
- Ensure that their computer's firewall is turned on.
- Inform the Parish Office of any breaches within 48 hours.