

THURSTON PARISH COUNCIL
Parish Council Office
New Green Centre
Thurston IP31 3TG

Tel: 01359 232854

e-mail: info@thurstonparishcouncil.gov.uk

website: <https://thurstonparishcouncil.uk/>



IT AND COMMUNICATIONS SYSTEMS POLICY - STAFF

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.

ABOUT THIS POLICY:

The Parish Council's IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards employees are expected to observe when using these systems, when the parish council will monitor their use, and the action it will take if staff breach these standards.

The Proper Officer has overall responsibility for this policy, including keeping it under review.

Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

EQUIPMENT SECURITY AND PASSWORDS:

Each member of staff is responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy. Passwords should be used on all IT equipment, particularly items that are taken out of the office. All passwords should be kept confidential and changed regularly.

Employees should only log on to the parish council's systems using their own username and password. They must not use another person's username and password or allow anyone else to log on using their username and password.

If an employee is away from their desk they should log out or lock your computer. At the end of each working day, they must log out and shut down their computer.

SYSTEMS AND DATA SECURITY:

An employee should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

Software from external sources must not be downloaded or installed without authorisation from the Proper Officer. Downloading unauthorised software may interfere with the parish council's systems and may introduce viruses or other malware.

No device or equipment including mobile phones, tablet computers or USB storage devices must be attached to our systems without authorisation from the Proper Officer.

Particular caution should be exercised when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

The Proper Officer should be informed immediately if you suspect a computer may have a virus.

COMMUNICATIONS FROM THE PARISH COUCNIL VIA E-MAIL:

- Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. The Parish Council's standard e-mail signature and disclaimer should be included in all emails sent.
- Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.
- Abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails should not be sent.
- Employees should not:
 - (a) send or forward private e-mails at work which they would not want a third party to read;
 - (b) send or forward chain mail, junk mail, or gossip;
 - (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or
 - (d) send messages from another person's e-mail address (unless authorised) or under an assumed name.
- Employees should not use your own personal e-mail account to send or receive e-mail for the purposes of our business.

USING THE INTERNET:

Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out under "Personal Use of Our Systems".

Employees should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

The Parish Council may choose to block or restrict access to some websites at its discretion.

PERSONAL USE OF OUR SYSTEMS:

We permit the incidental use of our systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use must meet the following conditions:

- (a) it must be minimal and take place substantially outside of normal working hours (that is, during your lunch break, and before or after work);
- (b) personal e-mails should be labelled "personal" in the subject header;
- (c) it must not affect your work or interfere with the business;

- (d) it must not commit us to any marginal costs; and
- (e) it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Procedure.

MONITORING:

Our systems enable us to monitor e-mail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

The Parish Council reserves the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- (a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;
- (b) to find lost messages or to retrieve messages lost due to computer failure;
- (c) to assist in the investigation of alleged wrongdoing; or
- (d) to comply with any legal obligation.

PROHIBITED USE OF OUR SYSTEMS:

Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

- (a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- (b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
- (c) a false and defamatory statement about any person or organisation;
- (d) material, which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);
- (e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of an employee's duties);
- (f) unauthorised software;
- (g) any other statement which is likely to create any criminal or civil liability (for the employee or us); or
- (h) music or video files or other material in breach of copyright.