

Holt Parish Council IT Policy

1. Introduction

Holt Parish Council henceforth known as “The Authority” recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. Everyone must adhere to this policy to maintain digital security.

3. Acceptable use of council provided IT resources and email

When using IT resources for the council’s purposes, you must adhere to ethical standards, and respect copyright and intellectual property rights.

Where possible, authorised devices, software, and applications will be provided by the Authority for work-related tasks.

You must not install unauthorised software without checking with the clerk, and you must not use equipment or email to access or forward inappropriate or offensive content.

4. What you must do if you use your own personal devices

The Authority will endeavour to provide the clerk with devices to use for council business.

When Councillors are using their own devices, you must make sure you are:

- using strong passwords for all your accounts
- downloading the latest operating system security updates
- using anti-virus software

5. Network and internet usage

You must be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

6. Password and account security

You are responsible for maintaining the security of your accounts and passwords. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

7. Email communication

The Authority will endeavour to provide you with an official email account for organisation-related communication only. If you are currently using a personal email account, you should aim to move over to an official email account as soon as practically possible. You must make sure that emails are professional and respectful in tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

8. Email access

The Authority reserves the right to check official council email communications done using the email address supplied by the authority to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they respond to FOI or subject-access requests. If you are using a personal email account for council business, this is still subject to data protections laws and FOI requests.

9. Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. You must regularly backup any important data to prevent data loss and follow the Parish Council's data retention policies.

You should retain and archive emails in compliance with this data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

10. Reporting security incidents

All suspected security breaches, including email breaches or incidents should be reported immediately to the Clerk of Holt Parish Council

11. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges.

12. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

13. Use of Social Media

The Parish Council will use social media in a safe, appropriate and purposeful way to engage and interact with the public, stakeholders, opinion formers and the media.

The Parish Council will abide by any relevant or applicable laws, terms, and conditions, so that the Parish Council is not exposed to risks.

The Parish Council's use of social media must be undertaken in accordance with the Council's Code of Conduct and IT Policy.

Use of social media sites will at all times be consistent with the Parish Council's duty to safeguard children, young people and vulnerable adults, in accordance with relevant statutory requirements and service specific protocols.

During the course of their work, Councillors and the Clerk to the Parish Council using social media sites for business purposes must maintain political neutrality and not indicate individual political opinions.

The reputation and / or business of the Parish Council, service users, partners or others connected with the Parish Council must not be brought into disrepute through use of social media sites.

The Parish Council social media accounts and its content will only be authorised by the Parish Council.

Councillors and the Clerk to the Parish Council must act in accordance with the law and be aware of the risk of legal action against them individually and the Parish Council if social media is used inappropriately.

14. Contacts

For IT-related enquiries or assistance, users can contact Clerk of Holt Parish Council.

All staff and councillors are responsible for the safety and security of IT and email systems.

Date of adoption: 19th March 2026 at a meeting of the authority on 19th March 2026 at a meeting of Holt Parish Council, see minutes of the meeting.

Date for next review: April 2027.