MALVERN TOWN COUNCIL

INFORMATION TECHNOLOGY USERS' POLICY

Reviewed by:	Policy and Resources Committee – 6 May 2026
Adopted:	Annual Council – 13 May 2026
Next review due:	May 2030

MALVERN TOWN COUNCIL

INFORMATION TECHNOLOGY USERS' POLICY

1. Introduction

Malvern Town Council henceforth known as "The Council" 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.

This policy should be read in conjunction with the Council's Data Protection and GDPR Policies.

2. Scope

2.1. This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. The authority endeavours to provide digital devices but acknowledges that some small members may be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Acceptable Use of Council Provided IT resources and email

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

3.2. To control the use of the Council's computer equipment the following will apply:

i. Only authorised employees should have access to the Council's computer equipment.

ii. Employees and councillors are personally responsible for the protection of council data and information which they use and access as part of their roles.

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

3.4. Employees and councillors must be careful about which Wi-Fi networks they join. and make sure they are using a trusted internet connection, which is password protected when carrying out official business

3.5. Individuals must not:

i. leave their user accounts logged in at an unattended and unlocked computer;

ii. perform any unauthorised changes to the IT systems or information;

iii. access, or attempt to access, data which they are not authorised to use or access;

iv. connect any unauthorised device to the council's network or IT systems;

v. store council data on any unauthorised equipment;

vi. give or transfer council data or software to any person or organisation outside of the Council without permission from the Town Clerk.

4. Use of Computer Equipment in the Offices

4.1. Employees are responsible for their own workstations and equipment which should be kept in good condition.

4.2. All computers must be password protected by a strong password, consisting of at least eight letters, and must include at least one upper case letter, a number and a special character. Passwords must be kept secure.

4.3. Employee-used computer equipment should remain on council premises unless permission is received from the Town Clerk for it to be used elsewhere.

5. Use of Computer Equipment for Home / Remote Working

5.1. Employees and councillors should ensure that they have authority from the Town Clerk before equipment is removed from the office.

5.2. Employees may use computer equipment when working from home as part of their agreed working arrangements or on a one-off basis as agreed with the Town Clerk. Remote working may also be required due to extreme weather, unsuitable conditions within the office or other significant factors and these will be considered and agreed with all staff on an individual basis.

5.3. Computer equipment must be securely stowed for transport purposes, should not be visible within the vehicle and must not be left unattended.

5.4. Computer equipment should only be retained outside of the office for the agreed period of home / remote working. The remote location will be the employee's home address unless otherwise agreed by the Town Clerk.

5.5. Employees working from home must be logged on to the Council's system at all times of their working hours.

5.6. This policy must be adhered to when working from home.

6. Internet access on council-owned equipment

6.1. The Council's employees are provided with internet access to assist with their job roles. The short and occasional use of the council's internet is permitted for personal use by employees if kept to reasonable limits which do not obstruct the productivity of the Council and if carried out during official break times.

6.2. The equipment services and technology that employees use as part of their job role are the property of Malvern Town Council. Therefore, the Council reserves the right to monitor how employees use the internet and email.

7. Use of council emails

7.1. Town Council email addresses are provided to employees and councillors for use in their respective roles.

7.2. Town Council emails should be restricted to council-related activities only. All data that is written, sent or received through the Council's computer systems is part of official records and therefore information contained in email messages should be accurate, appropriate, ethical and legal.

7.3. Employees and councillors must use their designated Town Council email address for all Town Council business. Private email addresses must not be used for Town Council business.

7.4. Employees and councillors must make sure that emails are professional and respectful in tone and must always check that confidential or sensitive information is being sent to the correct recipients.

7.5. 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.

7.6. The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Officers may need to access emails so that they respond to FOI or subject-access requests.

7.7. The following are not deemed acceptable:

i. distributing, disseminating or storing images, text or materials that are illegal or might be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person;
ii. forwarding council confidential messages or information to external locations;
iii. broadcasting unsolicited personal views on social, political, religious or other non-council related matters.

7.8. Employees and councillors should regularly review and delete emails when they are no longer required. Emails should not be kept longer that they are required in line with the

Council's Data Retention Policy. All employees and councillors should be alert to the characteristics of spam and phishing emails and should not reply to those emails.

7.9. Emails sent must have an appropriate disclaimer relating to the use of the information within the email.

7.10. Email messages should only be sent to those for whom they are relevant and must not be used as a substitute for face-to-face communication, or for the exchange of gossip.

7.11. All devices used to access the Council's emails should be password-protected and care should be taken so that they are not left unattended or could be read by unauthorised individuals.

7.12. Employees may only use non-council owned equipment to access council emails with the express permission of the Town Clerk.

8. Use of internet on Council-Owned Equipment

8.1. Employees should not access personal email mailboxes from council-owned equipment.

8.2. The following are deemed unacceptable:

i. visiting illegal or fraudulent sites;
ii. using the internet to send offensive or harassing material to other users;
iii. revealing confidential information about the Council in a personal online posting, upload or transmission;
iv. publishing defamatory and/or knowingly false information about any aspect of the Council in any format.

9. Social media

9.1. Social media posts should be professional and respectful in tone and should only be used in accordance with Malvern Town Council's Social Media Policy.

10. General

10.1. Whilst using the council's IT equipment and software, the following is not permitted:

i. sending or posting discriminatory, harassing or threatening messages, images or other content;
ii. using the organisation's time and resources for personal gain;
iii. violating copyright law;
iv. failure to observe licensing agreements;
v. sending or posting messages or material that could damage the organisation's image or reputation;
vi. sending or posting messages that defame or slander other individuals.

10.2. Violation of the law or any aspect of Malvern Town Council policy will result in disciplinary action.

11. Support and security

11.1. Employees should not interfere with the everyday running of the council's information technology systems, unless asked to do so.

11.2. Employees should ensure that all updates are installed regularly and no later than 48 hours after the advisory notice is seen.

11.3. Employees or councillors experiencing any problems with Town Council hardware, software or emails should contact the PA to the Town Clerk or in their absence the Operations and Office Co-ordinator, who will refer the issue to the Council's IT support contractors.

11.4. All suspected security breaches, including email breaches or incidents should be reported immediately to The Town Clerk.

12. Training and Awareness

12.1. The Council will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. You should engage in regular training on email security and best practices.

13. Compliance and Consequences

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