MALVERN TOWN COUNCIL

INFORMATION TECHNOLOGY USERS' POLICY

Reviewed by:	Policy and Resources Committee 21 March 2023
Adopted:	Full Council – 13 April 2023
Next review due:	April 2027

MALVERN TOWN COUNCIL

INFORMATION TECHNOLOGY USERS' POLICY

The objective of this policy is to ensure that all employees and councillors using Malvern Town Council (hereafter known as 'The Council') information technology systems have a clear understanding of what is permitted with the aim of ensuring the appropriate use of the Council's equipment, the safeguarding of IT systems and data and to ensure compliance with the Data Protection Act.

1. Use of computer equipment in the office

1.1. 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.

1.2. 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.

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

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

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

2. Use of computer equipment for remote working

2.1. Employees and councillors should seek authority from the Town Clerk before equipment is removed from the office.

2.2. Computer equipment must be stowed in the boot of a vehicle for transport purposes and must not be left unattended in the vehicle.

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

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

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

3. Internet access on council-owned equipment

3.1. 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.

3.2. 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 and the right to find and read any data that employees write, send or receive through council online connections.

4. Use of council emails

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

4.2. 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.

4.3. 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.

4.4. 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.

4.5. Employees and councillors should regularly delete or archive 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.

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

4.7. 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.

4.8. 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.

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

5. Use of internet on council-owned equipment

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

5.2. 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.

6. Social media

6.1. Social media should only be used in accordance with Malvern Town Council's Social Media Policy.

7. General

7.1. 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.

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

8. Support and security

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

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

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

8.4. Annual training will be made available to employees and councillors in respect of cyber security.