Information Technology (IT) and Cyber Security Policy

This policy sets out how the council manages its Information Technology and Cyber Security.

The policy is overseen by the Finance and GP Committee.

1. Introduction

1.1 West Moors Town Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.

1.2 The Town Clerk is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

2. General Principles

2.1 All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Town Clerk.

2.2 As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

2.3 All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & Retention Policies'.

2.4 All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason.

2.5 All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.

2.6 All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Town Clerk.

3. Training and Guidance

3.1 Employees will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

3.2 Members will be provided with access to cybersecurity training via the DAPTC.

4. General IT Policy

Employees

4.1 All employees will be assigned a council email address as appropriate.

4.2 Personal use of Council IT equipment is permitted but should be kept to a minimum during working hours. Reasonable use of the internet during working hours is permitted.

4.3 The council reserves the right to monitor all activity on company devices. This includes email activity and internet usage for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring usage will mean processing personal data.

Members

4.4 All members will be provided with a council e-mail address and must use this for all council business.

4.5 Members are reminded that any e-mail sent or received in their capacity as a Town Councillor is Council data and any e-mails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes e-mails on Personal Accounts when acting as a Councillor.

4.6 A copy of all e-mail sent from councillor e-mail accounts on the webmail is kept on the server; it is recommended that members not using webmail to access e-mail should set up a rule to ensure a copy of e-mail is kept on the server.

4.7 Members using social media in their capacity as councillors must make it clear they are speaking in a personal capacity and not representing the view of the council.

4.8 Members should ensure they are adhering to the Council's code of conduct when using social media.

4.9 Members must ensure that any personal devices used to access council systems (including email, websites and data) are password protected and access is restricted solely to the member.

5. Websites and Social Media

5.1 Officers shall ensure that any websites operated by the council are regularly reviewed to ensure content is accurate and up-to-date. Websites shall also be monitored for unauthorised access and abuse.

5.2 Council social media accounts will be operated by officers.

5.3 All council social media messages must be non-political, uncontroversial and used to promote/highlight the Town.

6. Password Protection

6.1 All council computers and systems must be password protected to prevent unauthorised access.

6.2 Where possible, two factor authentication should be utilised.

6.3 Users should ensure that unattended devices are password protected.

6.4 Passwords must confirm to the following criteria:

- Minimum eight characters
- Comprise at least one upper case letter, one lowercase letter, one number and one special character

6.5 Where possible, generic user accounts should be avoided.

6.6 Where users have unique access permissions and/or accounts for systems, these must not be shared with other users

6.7 Different passwords should be used for different devices and accounts.

6.8 Regular password changes are encouraged to enhance security.

7. Portable Devices

7.1 All portable devices must be protected to prevent unauthorised access. This can be by use of passwords, passcodes or other biometric measures as applicable.

7.2 Passcodes must be appropriate for the device and the level of risk that unauthorised access poses to the organisation; where devices can access council data or other systems, passcodes must be unique and not easily guessable.

7.3 Removable media (USB sticks etc) must not be used to store council data.

8. Incident reporting

8.1 All members and employees must report any incidents which could pose a risk to the council's systems or data security to the Town Clerk without delay. This includes but is not limited to:

- Lost devices
- Potential risk arising from phishing emails/websites
- Passwords having been shared
- Unauthorised access to systems

9. Misuse of IT

9.1 IT systems will be monitored for misuse and all misuse is prohibited.

9.2 Misuse includes, but is not limited to:

- Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material
- Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of defamatory material
- Transmission of material which in anyway infringes the copyright of another person
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
    - Wasting staff effort or networked resources
    - Corrupting or destroying another users' data
- Violating the privacy of other users
- Disrupting the work of other users
- Other misuse of the networked resources by the deliberate introduction of viruses/malware
- Playing games during working hours
- Altering the set up or operating parameters of any computer equipment without authority.

9.3 Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited

Adopted	10.07.2025	
Reviewed		