



Newhaven Town Council

IT AND CYBERSECURITY POLICY

Purpose of this policy	2
The scope of this policy	2
General Principles	2
Training and guidance	2
Policy	2
Employees/Volunteers	2
Councillors	3
Websites and social media	3
Password protection	3
Portable devices	4
Incident reporting	4
Misuse of I.T.	4

Purpose of this policy

Newhaven Town Council (NTC) 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.

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

Line managers have a responsibility to ensure that the staff they supervise comply with this policy.

The scope of this policy

It applies to all staff, whether full time, part time or temporary workers and to Councillors.

General principles

- 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. As a 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.
- All employees, members and other users of NTC IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & Retention Policy'.
- All NTC devices will have up-to-date antivirus software installed, and this must not be switched off for any reason without the authorisation of the Town Clerk.
- 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.
- All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Town Clerk.

Training and guidance

- Employees and volunteers will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.
- Councillors will be provided with a brief overview of cybersecurity measures as part of induction and may be provided with more in-depth training as required.

Policy

Employees/Volunteers

- All employees will be assigned a council email address as appropriate. Volunteers may also be assigned a council e-mail address where necessary.
- Personal use of NTC IT equipment is permitted but should be kept to a minimum during working hours. Reasonable use of the internet during working hours is permitted.
- NTC reserves the right to monitor all activity on company devices. This includes monitoring of clocking in and out, 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.

Councillors

- All Councillors will be provided with a council e-mail address and must use this for all council business.
- Councillors are reminded that any e-mail sent or received in their capacity as a Town Councillor is NTC 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.
- A copy of all e-mail received on the councillor e-mail accounts is kept on the server in line with the council's Data Protection and Retention Policy.
- 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.
- Councillors 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 NTC.
 - Councillors should ensure they are adhering to the NTC's code of conduct when using social media.
- Councillors 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.

Websites and social media

- Officers shall ensure that any websites operated by NTC are regularly reviewed to ensure content is accurate and up to date. Websites shall also be monitored for unauthorised access and abuse.
- NTC social media accounts will be operated by officers. The Town Mayor's official social media accounts may also be operated by the Town Mayor.
- All NTC social media messages must be non-political, uncontroversial and used to promote/highlight Newhaven.
- Approval must be obtained from the Town Clerk prior to the creation of any NTC websites or social media accounts.

Password protection

- All NTC computers and systems must be password protected to prevent unauthorised access.
- Where possible, two-factor authentication should be utilised.
- Users should ensure that unattended devices are password protected.
- Passwords must confirm to the following criteria:
 1. Minimum eight characters
 2. Comprise at least one upper case letter, one lowercase letter, one number and one special character
- Where possible, generic user accounts should be avoided.
- Where users have unique access permissions and/or accounts for systems, these must not be shared with other users
- Different passwords should be used for different devices and accounts.
- Passwords should be routinely changed.
- Passwords should not be written down or left in unsecure locations.

Portable devices

- All portable devices (including tablets and mobile phones) must be protected to prevent unauthorised access. This can be done by use of passwords, passcodes or other biometric measures as applicable.
- Passcodes must be appropriate for the device and the level of risk that unauthorised access poses to the organisation; where devices can access NTC data or other systems, passcodes must be unique and not easily guessable.
- Particular care must be taken when using removable media to transmit data as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents or data which could impact on the rights or reputation of any person or organisation including NTC) placed on removable media must be suitably password protected or encrypted.

Incident reporting

- All Councillors, employees or volunteers must report any incidents which could pose a risk to NTC's systems or data security to the Town Clerk, their deputy or the Chair of NTC without delay. This includes but is not limited to:
 1. Lost devices
 2. Potential risk arising from phishing emails/websites
 3. Passwords having been shared
 4. Unauthorised access to systems
 5. Harassment of other users

Misuse of I.T.

- IT systems will be monitored for misuse and all misuse is prohibited.
- Misuse includes, but is not limited to:
 1. 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
 2. Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
 3. Creation or transmission of defamatory material
 4. Transmission of material which in anyway infringes the copyright of another person
 5. Transmission of unsolicited commercial advertising material to networks belonging to other organisations
 6. Deliberate actions or activities with any of the following characteristics:
 7. Wasting staff effort or networked resources
 8. Corrupting or destroying other users' data
 9. Violating the privacy of other users
 10. Disrupting the work of other users
 11. Harassment of other users
 12. Other misuse of the networked resources by the deliberate introduction of viruses/malware
 13. Playing games during working hours
 14. Altering the set up or operating perimeters of any computer equipment without authority.
 15. Unauthorised access, use, destruction, modification and/or distribution of NTC information, systems or data is prohibited.

Date of policy:	22/11/2024
Approving committee:	Full Council
Date of committee meeting:	14/01/2025
Supersedes (name of old policy and reference):	N/A
Policy version reference:	AUITC01
Policy adopted by Full Council on:	14/01/2025
Date for next review:	January 2026