Newark
TOWN COUNCIL

IT Policy

August 2024

Content

INTRODUCTION

Newark Town Council has a duty to ensure the proper security and privacy of its computer systems and data. All users are responsible for protecting these assets.

The Town Clerk is responsible for implementing and monitoring this policy but may delegate that responsibility to another officer. Line managers are responsible for ensuring that staff comply with this policy.

GENERAL PRINCIPLES

All employees, members, and other users should be aware of the increasingly sophisticated frauds and cybersecurity risks and, when in any doubt, seek guidance from the Town Clerk. As a general rule, users should not be asked to share passwords via email, and they should be wary of unusual language in emails that may indicate a fraudulent message.

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 Policy.' All council 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 constitutes 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 receive regular cybersecurity training appropriate to their roles and level of system access. Members 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.

EMPLOYEES AND VOLUNTEERS

All employees will be assigned a council email address as appropriate. Volunteers may also be assigned a council email address as needed. 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.

The council reserves the right to monitor all activity on company devices. This includes email activity and internet usage to ensure compliance with our policies and procedures and with relevant regulatory requirements. Information acquired through

such monitoring may be used as evidence in disciplinary proceedings. Monitoring usage will mean processing personal data.

MEMBERS/COUNCILLORS

All members will be provided with a council e-mail address and must use this for all council business. Members are reminded that any e-mail sent or received in their capacity as a Town Councillor is regarded as Council data, and as such, e-mails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes emails sent from Personal Accounts when acting as a Councillor.

A copy of all correspondence received in the councillor's email accounts is retained on the server, in line with the council's Data Protection and Retention Policy. A copy of all correspondence sent from councillor e-mail accounts via webmail is retained on the server. It is recommended that members who do not use webmail to access email set up a dedicated drive to ensure emails are stored.

in a secure location.

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. Members should adhere to the Council's code of conduct when using social media.

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.

For more information, please refer to the Social Media and Code of Conduct Policies

WEBSITES AND SOCIAL MEDIA

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, and Council social media accounts will be operated by officers.

All council social media messages must be non-political, uncontroversial, and used to promote/highlight the Town. Approval must be obtained from the Town Clerk prior to the creation of any council websites or social media accounts.

For more information, please refer to the Social Media Policy

PASSWORD PROTECTION

All council computers and systems must be password-protected to prevent unauthorised access, and where possible, two-factor authentication should be used.

Users should ensure that unattended devices are password-protected. Passwords must conform to the following criteria:

- Minimum eight characters
- 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 using 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 council data or other systems, passcodes must be unique and not easily guessable.

Particular care must be taken when using portable devices to transmit data, as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents, or data that could impact the rights or reputation of any person or organisation, including the council) stored on portable devices must be password-protected or encrypted.

BRING YOUR OWN DEVICE (BYOD)

BYOD Introduction

Newark Town Council grants Councillors the use of smartphones and tablets of their choosing for council business. This policy is intended to protect the security and integrity of personal data controlled and processed by Newark Town Council. Newark Town Council reserves the right to revoke this privilege if Councillors do not abide by the policies and procedures outlined below. Councillors must agree to these terms and conditions.

Devices and Support

• Smartphones, including iPhone, Android, Blackberry and Windows phones, are allowed

• Tablets, including iPad and Android, are allowed

• Laptops are allowed

• Connectivity issues may be supported by ICT services, but this will be on a case by case. In the first instance, the connectivity issue should be reported to the Town Clerk.

• The device manufacturer or their carrier should be contacted for operating system or hardware related issues.

Security – Bring Your Own Device

• In order to prevent unauthorised access, devices must be password-protected using the features of the device and a strong password is required to access the Town Council network.

• Passwords must be at least six characters and a combination of upper- and lower-case letters with a number and a symbol.

• Passwords must be kept confidential and must not be shared with family members or third parties.

• Passwords must be changed if they are disclosed to another person or discovered.

• Devices must be encrypted.

• The device must lock itself with a password or PIN if it is idle for five minutes.

• Home Wi-Fi networks. Caution is advised when using public Wi-Fi networks, as they may not be secure.

• Public data backup and transfer services (Dropbox, Google Drive) must not be used.

• Data must only be stored on internal memory, never on a removable memory card.

• Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

• All data relating to Newark Town Council will be erased at the end of a Councillor's term.

• All data relating to Newark Town Council will be erased if there is a personal data breach

• All data relating to Newark Town Council will be erased if there is a virus or similar threat to the security of data.

Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using Wi-Fi facilities in public places (e.g. coffee shops or airports), or apps for smartphones and tablets, which may be capable of accessing sensitive information.

Risks/Liabilities/Disclaimers

Lost or stolen devices must be reported to Newark Town Council within 24 hours of being discovered. Councillors are responsible for notifying their mobile carrier immediately upon the loss of a device. Councillors must adhere to the Newark Town Council's BYOD policy as outlined above and are personally liable for all costs associated with their device.

Newark Town Council reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

MONITORING

The Council may, from time to time, monitor the Facilities. Principal reasons for this are to:

• detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies, including the health and safety, ethical and sex discrimination policies.

• ensure compliance with this policy.

• detect and enforce the integrity of the facilities and any sensitive or confidential information belonging to or under the control of the Council.

• ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time; and

• Newark Town Council has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be conducted in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 and the 2018 GDPR.

This policy must be read in conjunction with:

• Computer Misuse Act 1990

• Data Protection Act 1998

• GDPR 2018

The Council will not (unless required by law): allow third parties to monitor the facilities (with the exception of an appointed IT supplier); or disclose information obtained by such monitoring of the facilities to third parties unless the law permits.

The Council may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.