Councillor ICT Policy

Version	1.0
Status	Draft
Date	October 2024
Service	ICT
Owner	Carol Thomas
Authorised By	
Publication Date	
Review Date	

1. Introduction

We live in an increasingly digital world and one which is also subject to growing digital threats. Councillors, by the nature of their role, are in the public domain and therefore targets of cyber criminals. It is essential that Councillors as users of council equipment are aware of the risks posed created by insecure equipment, software and practice.

This policy is intended to help Councillors take the necessary actions to reduce the risks, and outlines the responsibilities and guidelines for councillors regarding the use of ICT resources provided by the council.

By adhering to this policy, councillors contribute to maintaining data security, efficient communication, and effective support.

2. Purpose of this policy

The purpose of this policy is to outline the technology equipment and services provided to Councillors and how to use these in a compliant manner which reduces risk to the council and the residents we serve.

3. Council ICT Equipment

The council will issue council-owned devices (e.g., laptops, tablets, smartphones) to Councillors for official use. A standard set of devices is available, selected to meet the needs of the majority of users and to keep costs down.

Council-issued devices remain the property of the Council and must be returned at the end of the councillor's term. Councillors must return Council owned devices within 48 hours of ceasing to be a Southend City Councillor.

Mobile devices are optional. If a mobile device is used by a councillor, it should be noted that numbers are not transferrable to members at the end of their term.

Council-issued devices will be automatically and remotely updated by the ICT team for security purposes. Should these updates fail for any reason, Councillors will be requested to return ICT equipment to officers in order for officers to perform the necessary updates or upgrades.

Councillors are responsible for the physical safeguarding and securing of devices issued. It is advised not to leave laptop bags on the seat in an unattended parked car, and to ensure that on trains the device is in view.

Council-owned devices will be replaced on a 3 or 4 year basis as part of the regular device replacement cycle. Any special needs equipment will be provided in line with Access to Work guidance

The Council does not provide broadband, printers or other peripheral devices.

4. Appropriate Usage

Council devices should be used for council matters and councillors should be aware that potentially sensitive data could be on their devices.

Councillors should use council issued ICT equipment for council business only and be mindful of any content shared. The costs of any damage or loss resulting from inappropriate use could be levied to Councillors.

Should Councillors use their own devices for Council matters, they must adhere to the security requirements set out in the 'Bring Your Own Device' section below.

5. Council Email and Outlook Calendar Usage

Email and Outlook Calendar provide a valuable communication, calendar and collaboration tool. This is a digital tool and subject to all digital risks and therefore particular care must be taken to ensure security of council data. Personal mail is not the topic of this policy, but councillors should ensure they are aware of the data risks inherent in personal mail.

Councillors must use their council-provided email accounts and not personal email for all official communication. Councillors should not forward official council emails to their private email addresses, and officers are discouraged from replying to Councillors email sent from private email accounts.

Personal email accounts should not be used for council business, as this could then expose the accounts to risk and potentially open them to Subject Access Requests. Therefore councillors are advised to be particularly aware of the risks of sharing confidential information via email.

Council calendars should not be merged with private calendars due to the risk of attached documents being shared in wider domains.

6. Security of Southend City Council devices

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

Passwords must be kept confidential and must not be shared with family members, employees or third parties. If a password has been disclosed to or discovered by another person, it should be changed.

Councillors should ensure that their Home Wi-Fi networks are encrypted for their security.

Councillors should exercise caution when using public WiFi networks as public Wi-Fi networks may not be secure.

Public data backup and transfer services (Dropbox, Google Drive, icloud etc) must not be used for council matters or documents for security reasons. Data must only be stored on internal memory, never on a removable memory cards.

If a Councillor experiences a personal data breach, a virus infection or similar threat to data security, Councillors must return the Council owned devices to Officers for assistance or on request.

Care must be taken to avoid using approved devices in a manner which could pose a risk to confidentiality and take care to avoid:

- clicking on links in suspicious emails;
- accessing potentially harmful websites;
- using potentially harmful application software (service desk will be happy to advise on acceptable software);
- using Wi-Fi facilities in public places (e.g. coffee shops or airports)

Rather opt to err on the side of caution or reach out to the ICT Service Desk for advice and guidance.

Any lost or stolen devices must be reported to the ICT Service Desk or Councillor Queries within 24 hours of discovering the loss.

7. Data Protection and Privacy

Councillors need to comply with data protection laws and the council's Data Privacy and Information Security. Personal data must be handled securely and only accessed for legitimate council purposes. Councillors need to be aware that special category data (e.g., health, ethnicity) requires additional care and protection.

8. Bring Your Own Device (BYOD)

Councillors may use personal devices (BYOD) to access council applications and data using the web versions of applications. The Council retains control over data accessed via BYOD and for this reason it cannot be downloaded to personal devices.

Should a personal device be lost, stolen or compromised, Councillors must report this to officers promptly so that Council data can be secured.

9. Service Desk Support

The Council's Service Desk is available for ICT support. This can be accessed via Councillor Queries, or directly via the Velocity Application.

Service Desk will assist in problem resolution, but it should be noted are not able to resolve connectivity issues that relate to Councillor's home broadband contracts.

10. Information and Cyber Security

To help keep the council and residents data secure, Councillors should use strong passwords, avoid sharing user names and passwords, avoid clicking on links in emails, and protect sensitive information following the guidance in this policy.

In the event of any suspected security incidents must be reported to Service Desk promptly so that these can be dealt with as fast as possible.

9. Compliance and Accountability

As councillors, we trust that you will accept and support the Council's work to keep resident data secure and comply with the requirements and spirit of this policy.

Please review this policy thoroughly, and if you have any questions or need clarification, feel free to reach out. Once you agree, please sign and return a copy to the ICT Director.

Councillor Signature : Date: