Members ICT Policy

January 2023

Contents

Members ICT Policy

Title: Members ICT Policy	**Approved**:	**Effective from**: Click here to enter a date.	**Next review**: 20/12/2025
Version: 1.01	**Author**: Cliff Dean		**Last review**: 22/12/202222

Version History

Revision Date	Reviser	Previous Version	Description of Revision
May 2019	Cliff Dean	1.0	Updated to reflect password changes
December 2022	Cliff Dean	1.01	Updated Policy reference IT and ICT, update personnel use, removed reference to tablet.

Document Approvals

This document requires the following approvals:

Sponsor Approval
West Lindsey - Corporate Policy and Resources Committee

Document Distribution

This document will be distributed to:

Name	Method
All members	Members Handbook

Notes: All roles listed above receive copies, or are notified, of updated versions of the document.

The Method of Issue includes provision of paper or electronic copy of authorised document, or notification by e-mail to those with access to the authorised version on the Intranet.

1. Introduction

West Lindsey District Council promotes the effective use of ICT technology by its Elected Members to enable them to perform their duties as a Councillor.

The Council's general presumption is for electronic provision of information and transaction of business wherever possible, while recognising that Councillors have different needs and requirements. By accepting a Council issued device, Members are asked to use the Council's ICT facilities to access Council information, including committee papers, to support a more sustainable approach by reducing paper consumption and postage usage, whilst improving timeliness in communication.

This policy applies to all Elected Members and Co-opted Members of the Council and aims to protect Members and the Council against legal challenge, criminal liability and damage to reputation. This is supported by four key objectives, which are:

- To prevent Council resources from being used to promote political activity;
- To prevent the Council's name from being used to promote a Member's personal or business interests;
- To protect the Council's private, personal and sensitive information from all threats, whether internal or external, deliberate or accidental;
- To prevent unnecessary cost being incurred by the Council.

The use of all ICT equipment, systems provided, or apps etc made accessible, by the Council is subject to this policy. Any Member wishing to use the Council's ICT equipment and/or systems is required to undertake in writing that they observe and will comply with this policy.

2. Members ICT Support

ICT support is provided for Members through Democratic Services at committeeadmin@west-lindsey.gov.uk or the ICT Team at the ICT ServiceDesk on 01427 675165 or via email ICT_ServiceDesk@sharedlincs.net.

To escalate any ICT issues or concerns, please contact the Council's Shared ICT Manager at Cliff_Dean@west-lindsey.gov.uk.

The Council will provide training opportunities at the Council's expense on all aspects of Council related use of the software/hardware provided by the Council.

3. Members ICT Provision

3.1 Council Issued Hardware

Members will be provided with a maximum of 2 devices for accessing systems, email, calendar, committee papers; etc. This can be used to access Council systems.

Due to advances in technology, alternative hardware may become available for use by Members. The Council retains the right to offer alternative hardware should the situation arise.

The devices provided by the ICT Section will be installed with the current standard software that will be configured to regularly update the device operating system.

The software and ICT equipment will be maintained, replaced and repaired as necessary at the Council's expense.

3.2 Members Own Hardware or Any Other Device

Members can be given access to use their own devices for accessing email on another device, subject to the device meeting the minimum-security requirements, this can be requested via the ICT ServiceDesk.

3.3 Access to Systems

Members will be provided with access to the Council's preferred choice of services and applications, e.g., OneDrive and Modern.Gov. The Council will download and set up the required applications and will notify you when there are updates to be applied. These will be applied remotely on the device provided by the Council.

3.4 Acceptable Use

Members will not be able to use Council provided ICT software and systems in connection with Council business on any personal device(s) apart from that defined in section 3.2..

Council business means matters relating to a Member's duties as an Elected Member, as a member of a Committee, Sub Committee, working party, or as a Council representative on another body or organisation.

Council ICT equipment is available to enable:

- Communications with individual Members of the public, other Members, officers, and government officials in connection with those duties set out above;
- To facilitate discussion by a political group of the Council, so long as it relates to the work of the Council and not the political party.
- Members must also note the General Principles in the Members Code of Conduct with particular regard to the following principles:
- Members should uphold the law and on all occasions act in accordance with the trust that the public is entitled to place in them;
- Members should do whatever they are able to do to ensure that the Council uses its resources prudently and in accordance with the law.

ICT equipment should not be used in a manner that breaches the Members' Code of Conduct. The Code makes it clear that when using the resources of the Council Members must:

Act in accordance with the Council's reasonable requirements;

- Ensure that such resources are not used improperly for political purposes (including party political purposes). This means that the use of the ICT equipment for purely party-political purposes, designing and distributing party political material produced for publicity purposes and support of any political party or group activities, elections and campaigning is likely to amount to a breach of the Code of Conduct;
- For any illegal activities which may bring the Council into Disrepute;
- For any purpose which is inconsistent with this policy.

The following do not constitute Council business and Council resources should not be used:

- Communications for constituency party meetings, ward party meeting, etc. or letters to party members collectively or in their capacity as party members;
- Documents relating to the policy and organisation of political parties, particularly regarding the conduct of elections.

3.5 Responsibilities of Members

There is an expectation that reasonable care is taken in the use and security of equipment. The Council may, at its discretion, require the Member to pay all or some of the cost incurred if loss or damage has resulted from their wilful neglect.

Security – reasonable care must be exercised in order to prevent theft, loss or damage at all times. Specifically, any mobile devices, e.g., tablets, must not be left unattended. An appropriate carrying case should be used to prevent damage to the equipment. All ICT equipment should be kept out of sight overnight in a secure location;

- Bit lockers should not be left in laptops(these are the usb keys used to secure a device).
- Transit – ICT equipment must be kept out of sight and secured in a locked boot where available. ICT equipment must not be left in sight in an unattended vehicle and must be removed from the vehicle overnight. When using hotel accommodation Members should consider the use of the hotel reception safe when a mobile device is not in use, and where not available, the use of a room safe or lockable cabinets within the room.

3.6 Restriction of Use

The Council reserves the right to restrict the use of ICT equipment if it has reason to believe that the use of the ICT equipment is likely to be in breach of the Council's IT Security Policy and supporting guidance. In particular, the Council reserves the right to:

- Remove or disable any software or equipment;
- Remove any information stored on the computer.

3.7 Return and Recovery of Equipment

All ICT equipment and software assigned remains the property of the Council. The Council reserves the right to require the Member to return the ICT equipment at any time and the right to recover the ICT equipment from the Member.

Any Member to whom ICT equipment has been supplied and ceases to hold office, for whatever reason, will be required to return all equipment to Democratic Services within two weeks of ceasing office. All information held on the equipment will be deleted and the equipment may be re-issued.

4. Members Personal Use

The ICT equipment provided for Members is intended to assist the Member in his or her duties as a Councillor.

Council ICT equipment may also be used for reasonable and appropriate personal use, for example, web browsing, email, if this does not degrade the performance of the equipment or contravene this policy, providing that the primary use of the equipment remains for conducting Council business. However, the downloading of any additional apps onto the device is prohibited.

Councillors are permitted to store personal information and files on the device. However, the Council accepts no liability or responsibility for the loss of any such data and Councillors should back up any valuable personal data. The loss of data can occur, for example, if the device fails or if the device is required to be rebuilt for any reason.

All of the ICT equipment and software provided to Members remains the property of the Council. Members therefore have an obligation to ensure that they:

- Take reasonable care to safeguard ICT equipment and software supplied;
- Follow the instructions given by the Council, authorised contractors and manufacturers of the equipment as to its use and not allow it to be interfered with;
- Protect ICT equipment against theft and unauthorised access;
- Do not modify the ICT equipment in any way; this includes any amendments to the hardware and software configuration;
- Maintain the ICT equipment in working condition and report any faults to the IT Section as soon as is reasonably practicable;
- Allow reasonable access to the equipment for regular inspection, maintenance, upgrades or remedial work;
- Otherwise, comply with the terms of this policy and any other Information Management Policy and IT Security Policy.

5. IT Security Considerations

When using Council provided ICT equipment it is necessary that Members comply with the Council's IT Security Policy requirements as below:

Email and Internet access is provided to Members as a means of improving communications, knowledge and effectiveness at work. Nevertheless, all usage of the Council's email and Internet facilities must be regarded as the property of the Council and should not be regarded as private.

Use of email and Internet access introduces security threats such as malicious code attached e.g., viruses, unsolicited or undesirable email, fraudulent attempts to acquire sensitive information such as passwords and credit card details, unauthorised content, and breaches of legislation e.g., computer misuse and copyright act.

The security of ICT equipment is the responsibility of each Member as its 'custodian.' Access to the Council's information systems via ICT equipment is subject to password security. Members must keep passwords secure, and they must be of adequate complexity as advised by the ICT Team.

6. Email Usage

The Council will provide Members with a Council email address which must be used for all emails when conducting, or in support of, official Council business.

Non-Council email platforms e.g., webmail, Hotmail, must not be used to conduct or support official Council business.

Members must ensure that any emails containing confidential or sensitive information must be sent from an official Council email.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Council business should be considered to be an official communication from the Council.

Under no circumstances should Members use email and Internet facilities for:

- Illegal or malicious use, including downloading or transmitting copyright material;
- Accessing, sorting or transferring illegal, pornographic or obscene material.
- Access to or distribution of material, which does not comply with the Council's Equality and Diversity policy;
- For potentially libellous or defamatory purposes.

7. Internet Acceptable Usage

The Council will provide access to the Internet through your network account which comprises a secure logon-id (username) (password). The Council's ICT Department is responsible for the technical management of this account.

You are responsible for the security provided by your network account. Only you should know your log-on id and you should be the only person who uses your account.

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- monitoring total usage to make sure business use is not impacted by lack of capacity; and
- monitoring and recording all access for reports that can be produced for the Monitoring Officer and auditors on request.

Except where it is strictly and necessarily required for your work as a Councillor, you must not use your Internet account to:

- create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive;
- subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files;
- subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs;
- subscribe to, enter or use online gaming or betting sites;
- subscribe to or enter "money making" sites or enter or use "money making" programs;
- run a private business;
- download any software; or
- use any material obtained from the Internet in a manner which might infringe the owner's copyright.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and material that is against the rules, essence and spirit of this and other Council policies.

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

Any Councillor found to have breached this Policy may be subject to investigation under the Members Code of Conduct. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

8. Information Security and Management

8.1 Confidentiality

Members accessing confidential Council information using Council provided ICT equipment are responsible for ensuring the continuing security of any such confidential information that they deal with.

Members are reminded of their obligations under the Council's Code of Conduct for Members not to disclose confidential information to any third party. Members are reminded that when conducting case work they are data controllers in their own right and must comply with data protection principles.

8.2 Legislative Framework

This policy was developed within a framework of legislation including, for example, the General Data Protection Regulations, Data Protection Act, Computer Misuse Act and Freedom of Information Act. It is expected that Members will safeguard any Council information in accordance with the Data Protection Act and Freedom of Information requirements.

More information about the relevant acts and regulations can be found in the Information Governance Policy or alternatively contact the Corporate Information Officer