COUNCILLORS' ICT USAGE AGREEMENT

This agreement should be read in conjunction with the Members' Code of Conduct and covers the core requirements for usage of ICT equipment and service provided by the Council.

Provision of ICT Equipment

Elected councillors can choose from a range of options as to how they access council services. Provision is via android tablet, ICT Provision in the Members' Room, or by remote access using their own computer. The option of a mobile / smart phone is available to executive councillors.

Training and Development

The Council will provide training opportunities at the Council's expense on all aspects of Council related use of the software/hardware. All councillors must complete the online Cyber Security and Data Protection training 'Cyber Ninja's for councillors' accredited by the National Cyber Security Centre on induction and updated annually. This training can be found of the Council's intranet Data Protection - Home (sharepoint.com).

Conditions of usage

In order to utilise Council provided ICT Equipment and services, the Council's policies must be observed. Key elements are outlined below. More information can be found in the Council's ICT Security and other policies including the Council's Data Protection Policy.

General

Acceptable Use

- Council ICT equipment is provided for councillors to use in connection with Council business only.

Insurance

- Security – reasonable care must be exercised in order to prevent theft, loss or damage at all times. Specifically, any mobile devices, for example laptops, must not be left unattended.

- Transit – ICT equipment must be kept out of sight and secured. Only leave in a locked car boot if there are no better alternative options.

- Travelling abroad – it is not envisaged that there will be a regular requirement to take Council provided mobile devices abroad. If there is a specific requirement, the councillor should seek advice from the Democratic Services and Elections Manager.

Privacy

- It is the policy of the Council that email and internet use will be monitored.

- Inappropriate use or content will be bought to the attention of the Monitoring Officer and may result in an investigation. Inappropriate use includes defamatory comments, swearing and abusive behaviour.

- All emails sent and received from a council email address are potentially disclosable to the public and press, for example, through information requests to the Council under the Data Protection Legislation (UK GDPR and the Data Protection Act 2018) and the Freedom of Information Act 2000.

Confidentiality

- Councillors may be able to access confidential Council information using the ICT equipment. Councillors are responsible for ensuring the continuing security of any such confidential information that they receive, including the security of any storage of such information on the computer or tablet.

- Councillors must ensure that no one else can view any personal details on the screen.

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 Councillor to return the ICT equipment at any time.

- If any councillor, to whom equipment has been supplied, ceases to hold office, for whatever reason, they will be required to return the equipment to Democratic Services within two weeks of ceasing office.

IT Security Policy

It is necessary that councillors comply with and have a working understanding of the Council's IT Security Policy and supporting guidance notes, which apply to all ICT equipment and systems. Below is an overview of the key points within the Policy.

Email and Internet Acceptable Usage Guidance

The Council's email and Internet facilities are intended for Council business use only.

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.

Non Council emails for example, Hotmail, must not be used to conduct or support official City of Lincoln Council business.

No forwarding of emails from council email addresses to personal email addresses will be permitted, either automatic or manual forwarding by officers or councillors.

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

i) illegal or malicious use, including downloading or transmitting copyright material; or
ii) accessing, sorting or transferring illegal, pornographic or obscene material.

Access to certain categories of website will be restricted for example for adult entertainment, drugs and alcohol or gambling (if access to a blocked site is required this can be overridden by contacting the IT helpdesk), subject to the site being used for appropriate council business.

All councillors are responsible for complying with the Council's Email and Internet Acceptable Use Guidance.

Remote Working Policy

Business critical data should be stored on a Council file and print server wherever possible and not held on the portable computer device.

No family members may use the IT equipment. The IT equipment is supplied for the sole use of staff or councillors.

The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, City of Lincoln Council may recover the costs of repair.

Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database or carry out any processing of information relating to the Council, its employees, or customers. **Under no circumstances** should Council information be emailed to a private non-Council email address. For further information, please refer to the Email Mandatory Guidance.

It is possible for staff and councillors to use their own computer for remote access into the Council's system. The computer must be up to date with a current and update antivirus product installed and active.

Information Protection

An incident is an event that could cause damage to the Council's reputation, service delivery or even an individual. This could be a lost laptop or paper case file, a virus on the network or a damaged piece of hardware.

Councillors should report any incidents or suspected incidents immediately by contacting the IT Section.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal data is information related to an identified or identifiable natural person who can be identified directly or indirectly by reference to an identifier such as a name.

Councillors should report any personal data breaches immediately to the Data Protection Officer or the Legal Services Manager or if both unavailable any member of the Legal Services team.

Councillors need to keep evidence of security breaches or system incidents; in case these are required later. In relation to personal data breaches Councillors will be required to complete an online data breach form if they have access to the Council's Hub (SharePoint) if not this will be completed on their behalf. This e-form is completed to record the incident and not to report it. As stated above any such breaches should be reported immediately by contacting the above-named officers.

Removable Media

It is the Council's policy to prohibit the use of all removable media devices. Removable media devices are electronic items usually used for storing or transporting data, for example a computer disk (CD or DVD), USB memory stick, MP3 player, external hard drive or a camera memory card. The use of removable media devices will only be approved if there is a valid business case for its use.

All data stored on removable media must be encrypted where possible.

Any removable media device that has not been supplied by the IT Section must not be used. All ICT equipment supplied will by default have removable media facilities disabled unless there is a valid business case.

Software

Councillors must not install or configure any software on the Council's ICT equipment. If a councillor requires any software for their council work, they must consult the IT Helpdesk.

All standard software installed on Council issued ICT equipment is correctly licensed and the Council will hold the details and records. These licences apply to a single copy of the software on one machine. The software must not be copied to any other machine.

No data should be entered onto internet-based services without prior approval by the ICT team.

Updates and maintenance

Periodic updates should be applied to any equipment supplied. Further guidance can be provided by the ICT team.

Responsibilities for Passwords

Councillors must follow the Council's Password Guidance in the selection and use of passwords.

It is the responsibility of all employees/users of the Council's IT systems to maintain password security. Ensure no passwords are issued to unauthorised personnel. Passwords should not be divulged for any purpose.

Reporting of and Managing IT Security Incidents

Incidents affecting IT security must be reported to the ICT Helpdesk as soon as possible.

As stated above, any personal data breaches must be reported immediately to the Data Protection Officer or the Legal Services Manager or if both unavailable a member of the Legal Services team.

Further information may be found on the Councils Intranet - Data Protection - Home (sharepoint.com) .

ICT Helpdesk

IThelpdesk@lincoln.gov.uk, 01522 87(3327)

Data Protection Officer

dpo@lincoln.gov.uk

01522 881188

COUNCILLOR AGREEMENT

I, Councillor . . . . . , have read and understood the Councillor ICT Policy as set out above and hereby agree to comply with the terms of the policy.

Signed:	
Date:	
In the presence of:	*(Officer of City of Lincoln Council)*
Signed:	