

ICT Acceptable Use Policy

Adopted by the Governing Body March 2025

To be reviewed March 2027

Policy overview

This policy sets out individual responsibilities which assist in protecting our information and communication technology (ICT).

Scope

The policy applies to:

- any individual using or accessing council ICT
- all council owned or leased ICT such as:
 - PCs
 - laptops
 - notebooks
 - smartphones
 - software
 - services
 - storage media
 - network resources

Training and awareness

You must undertake annual information assurance training. This is provided via the council's E-learning platform.

You must comply with any other obligations that we make you aware of including:

- legal
- statutory
- contractual
- policy

General responsibilities

You must:

- protect your username, password, and security token against misuse
- operate a clear screen policy when you leave your computer unattended. This can be done by, for example, "locking" the computer by:
 - pressing the ctrl, alt and delete keys simultaneously
 - clicking the "Lock Computer" button on the screen
- prevent inadvertent disclosure of information and avoid being overlooked when working

- protect hard copy material, portable devices, and removable media at all times. You must ensure they remain accounted for. When not in use you must secure them under lock and key
- ensure all removable media and portable ICT are encrypted
- securely destroy printed material and removable media when no longer required
- only access or attempt to access ICT you have been authorised to access
- only access or attempt to access information for official council purposes aligned with your role. This must be on a need-to-know basis
- connect council ICT such as desktops and laptops to the council network at least once every 30 days or it may be disconnected. To reconnect you must call the Service Desk on telephone number 01522 555555
- connect council ICT such as desktops and laptops to the council's network continuously for at least six hours per month to receive security updates. This can be directly or remotely via AOPVN. You must ensure devices remain connected until updates have been received and applied, for example Windows updates

Unacceptable use

You must not:

- use the username and password of another person
- share your own username and password with another person
- misuse, bypass, or subvert the configuration or security settings of any ICT
- introduce unauthorised software, hardware, removable media, or files
- process or access inappropriate material, including:
 - racist
 - sexist
 - defamatory
 - offensive
 - obscene
 - illegal
- carry out illegal, fraudulent, or malicious activity
- use ICT to carry out or support business which is unrelated to the council
- break copyright or carry out any activity that negatively impacts intellectual property rights

Email

You must:

- only transmit emails from your own authorised account
- check that the recipients of e-mail are correct to avoid accidental release to unintended recipients. Care must be taken when using auto complete to avoid the inclusion of an unintended email address
- password protect attachments which contain personal data or other sensitive information to mitigate the risk of sending an email to an incorrect recipient
- use the blind carbon copy (BCC) feature when sending an email to more than one recipient and it is necessary to protect email addresses. An example of this could be when sending an external email to multiple members of the public or multiple suppliers

You must not:

- auto-forward council email (@lincolnshire.gov.uk) to a non LCC corporate email address as security of alternative email addresses cannot be assured
- use personally owned email accounts to conduct official business or to transmit or receive council information

Malicious email:

- do not open an attachment, click on any link, or respond to an email unless you are confident the email is legitimate
- only release quarantined email if you are confident it is legitimate
- do not forward a suspicious email unless instructed to do so by the Service Desk
- if in doubt about an email or if you think you have received a malicious email, such as a phishing email, or an email containing malicious software, report it to the Service Desk on 01522 555555 immediately

Personal use of corporate email shall be:

- reasonable
- proportionate
- occasional

It must not interfere with the performance of your role or the performance of the system.

Delegate access

Delegate access to email accounts must only be provided following a clear business need. This must be authorised by the email account owner, or, in their absence, an appropriate senior manager.

Delegate access must not be provided by supplying details of a user's credentials, for example username and password.

When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must:

- not open it
- stop immediately if the email has been opened

Internet usage

You must not:

- use unofficial internet services, resources, or applications to process council information unless you are content for the information to be in the public domain
- use unofficial internet services resources or applications to process council owned personal data or information which is commercially, politically, or financially sensitive
- engage in activities that could compromise the security of our systems or data
- download, access, or share any illegal, offensive, or inappropriate content
- visit internet sites that contain obscene, hateful, pornographic, or otherwise illegal material
- download unauthorised software onto our Network
- use the Internet for personal financial gain

You must:

- ensure personal use of the internet is reasonable, proportionate, and occasional and must not interfere with your role
- respect intellectual property rights, including copyright, when downloading or sharing content from the internet
- report any suspected security incidents, or unusual or unexpected behaviour to the Service desk immediately
- use Artificial Intelligence services in line with the council's Artificial Intelligence policy

Passwords

Self-generated passwords must not be easily guessable for example 'letmein123', 'Password1'. They should not consist of keyboard patterns or sequential numbers for example qwerty, 12345.

You must protect passwords from unauthorised disclosure.

You must not record passwords unless it is done so securely, and you are the only one who can access it.

You must not use the same password across different accounts (work and private) and, or applications.

Software and hardware default passwords must be changed.

You must register for the corporate password self-reset function. If you do not and you require a password change you must be prepared to identify yourself when contacting the IT service helpdesk.

Removable media

You must only use removable media when absolutely necessary. It must be encrypted. Removable media includes:

- CDR
- DVDR
- Portable hard drives
- USB stick

You must not introduce removable media from an unknown source to our ICT.

You must always keep passwords used to authenticate removable media separate from the media.

When removable media is no longer required you must return it to the issuing department, or securely destroy it.

Bluetooth

Bluetooth can be used to connect to council devices. When not in use you must turn it off. This can be achieved via settings on your laptop or desktop.

Only connect via Bluetooth to authorised devices such as those in the IMT service catalogue. If you have been authorised to connect to another device only use Bluetooth devices that display the Bluetooth trademark.

You must not pair new Bluetooth devices in public spaces.

You must not accept files transmitted via Bluetooth from unknown or suspicious sources.

You must reject any pairing requests from unknown devices.

Remote or mobile working

You must take additional care when working outside of official premises. You must apply appropriate and reasonable safeguards to manage the increased likelihood of loss or compromise.

You must only remove ICT, removable media, and hard copy information from official premises when there is a clear business need.

You must only store ICT, removable media or hard copy information in an unoccupied vehicle if it is secured out of sight in the locked boot of the vehicle and only if the alternative option is less secure. For example, when entering a service users home.

You must not store passwords and security tokens with ICT at any time.

You must never store ICT, removable media, and hard copy information in a vehicle overnight.

Bring your own device

Bring Your Own Device (BYOD) means using your personally owned device to access council data.

You must use one of our supported BYOD solutions:

- accessing Microsoft 365 through a web browser
- accessing Microsoft 365 applications on your device using our BYOD software.

BYOD is optional. Your device must meet certain criteria before being allowed to access our data.

Technical support will be limited to our BYOD software and systems.

To ensure security of the device and council data is maintained, we may monitor usage of BYOD devices. Monitoring includes:

- the make and model of devices in use
- the version of the operating system currently installed

Devices which no longer meet the expected criteria will result in BYOD services being withdrawn.

To use BYOD software, you must allow the installation of council-controlled software. Corporate controls are restricted to council-owned data and managed services only, for example:

- remote wiping of council data and apps
- access revocation to council data

To ensure additional risks are managed, technical controls are in place. These controls may prevent you from undertaking some activity, for example restrictions on the transfer of council data out of the BYOD software.

You will be required to undergo multi-factor authentication.

We retain ownership and responsibility for the data.

You must:

- ensure access to your device is controlled by using a password or a PIN
- keep your device and system passwords secure
- use biometric features on the device, where possible
- have automatic device lockout enabled
- keep your operating system and software updated
- encrypt your device
- ensure you are not overlooked when using the device
- report lost or stolen devices as soon as possible to the IT service desk
- inform the IT service desk if you leave the council
- inform the IT service desk if your device is:
 - infected with malicious software
 - subject to a cyber-attack

You must not:

- share your passwords

- make copies of data or take screenshots
- attempt to bypass security controls or modify BYOD software
- jailbreak or root your device
- try to access systems for which they are not authorised

Monitoring

We reserve the right to monitor council communication systems and services. This includes, but is not limited to:

- email
- telephone conversations
- electronic messaging
- internet use
- system access

We use monitoring for the following purposes:

- to maintain and ensure security of systems and information
- to check for unauthorised use
- to establish facts relevant to council business
- to ensure quality assurance and ensure that procedures are being followed
- to undertake disciplinary, performance, and capability proceedings
- to prevent or detect crime
- to ensure the council remains compliant with the regulatory and legislation framework in force at the time

Reporting security incidents

You must report all security incidents, including near misses and suspected security incidents, in accordance with our [security incident policy](#).

You must report all security incidents involving ICT to:

- the service desk on telephone number 01522 555555
- our [Information Assurance Team](#)

You must report all other security incidents to our [Information Assurance Team](#). If you are a Serco employee you must report incidents to your security manager.

Breaches of policy

All council staff have a contractual responsibility to be aware of, and conform to, our:

- values
- rules
- policies
- procedures

Breaches of policy may lead to staff going through our disciplinary procedure in accordance with our [Code of Conduct](#) and [disciplinary policy](#).

Non-council staff may have their access to council information and, or ICT revoked.

Further information

For further information please email IA@lincolnshire.gov.uk.