Acceptable Use of ICT Policy

Version 3.1 (22 January 2021)

Author	*Rob Leitch*	**Contact details**	*LeitchRo@northlan.gov.uk*
Owner	*Senior Information Risk Officer*		*LeitchRo@northlan.gov.uk*

Date	*22/01/2021*	**Version number**	3.1	**Document status**	*Final Version*

Governance Committee	*Finance and Resources Committee*	**Date approved**	*11 March 2021*
Review date	*January 2023*		

Strategic Alignment:*Improving the Council's Resource Base – A Workforce Strategy that is built around the needs of the Council (as a single resource base) to deliver the priority outcomes, ensuring future workforce requirements, new skills and innovative approaches, and succession planning are recognised.*

Consultation process	*Consultation with stakeholders carried out June 2020 to January 2021*	
Stakeholders	*All Employees*	
	Joint Trade Unions *JNC for Teaching Staff*	
Distribution	*Available on myNL*	

Change record

Date	*22 January 2021*	**Author**	*Karen MacFarlane, Digital Services Manager*
Change made	*Updated to reflect current data protection and legislative requirements for the use of ICT within organisations*		

LIVE
LEARN
WORK
INVEST
VISIT

Foreword

We ASPIRE that North Lanarkshire is **the** place to Live, Learn, Work, Invest and Visit. This means we must respond to, and embrace, major social, economic, and technological change.

The Digital and IT Strategy brings together separate but related plans and policies that contribute to the development and delivery of our digital vision. The Acceptable Use of ICT Policy is a sub policy of this strategy. It provides a safe framework for using ICT without exposing the council or our employees to risks.

The policy supports the Employee Code of Conduct which sets out the standards of conduct to which every employee must adhere. Following this code and the details within the ICT Acceptable Use Policy will ensure that the standards set by the council are met.

1. Introduction

North Lanarkshire Council invests substantially in information technology and communication (ICT) systems that help employees to work flexibly and efficiently. The purpose of this policy is to provide the council's ICT users with guidance on the appropriate use of technology including, but not restricted to, email, internet, PCs/laptops, mobile/smartphones and tablets, social media and shared network drives/Microsoft Office 365. It applies to council devices as well as personal devices when accessing council systems and data e.g. NL Life.

The policy supports the need to keep the council's ICT estate in a safe and effective operational state to ensure the confidentiality, integrity and availability of information.

2. National Context

The council complies with all relevant legislation including (but not limited to) the following.

- Human Rights Act 1998
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Public Records (Scotland) Act 2011
- Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping purposes) Regulations 2018
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002

3. Scope

This policy applies to users of council ICT assets including employees, elected members, contractors, consultants, temporary agency staff, modern apprentices, students, volunteers and personnel affiliated with third parties.

Individuals using the schools' network and public access through libraries have separate guidelines covering acceptable terms and conditions of use. Elected Members have separate guidelines covering various aspects of conditions of use.

'ICT assets' refers to any council provided equipment and systems such as: physical hardware, software applications, peripherals and components of the council's network infrastructure that support the transmission of electronic data. This applies regardless of where equipment or systems are located and used.

4. Overview

Authorised users will be granted access rights to council ICT facilities appropriate to their business requirements. No unauthorised facilities should be used.

Authorised access to ICT facilities is taken as acceptance of this Acceptable Use Policy and that all computer use shall comply with relevant legislation.

While access to ICT facilities is provided for business use, reasonable personal use may be undertaken. Any personal use must comply with relevant council policies, must not interfere with normal business or be detrimental to productivity.

To ensure ICT facilities and services are operating efficiently and effectively, usage data will be collected and recorded. This will include use of email and internet facilities. While monitoring of individuals will not happen as a matter of routine, personal information may be accessed as part of the procedure. Where personal use of council facilities is undertaken there can be no presumption of privacy.

Where there is a suspected breach of this policy the council will take the appropriate steps in accordance with relevant investigatory and/or disciplinary procedures. Suspected unlawful acts will be referred to the appropriate authorities.

5. Appropriate use of Council Technology and Systems

All employees are expected to adhere to the standards set out in this document, the Information Security Policy and all related guidance. All information stored on council systems and network is corporate property and should be regarded as such.

IDs and passwords

Users will:

- Protect usernames, employee reference numbers and passwords
- Create secure passwords following best practice
- Not log onto any council systems using another user's credentials
- Lock their screen when temporarily leaving devices in use (press control + Alt + Del and select lock from a PC/laptop)
- Log out of all council devices when not in use

Managing and Protecting Information

Users will:

- Understand that they, and the council, have a legal responsibility to protect personal and sensitive information
- Ensure that all information is created, used, shared and disposed of in line with business need and complies with the council retention schedule and information governance policy framework
- Not access personal data unless there is a valid business need that is appropriate to their job role
- Not provide information in response to requests from people whose identity they cannot verify
- Be careful not to be overheard or overlooked in public areas when conducting council business

Using social media for business

The council has guidance for authorised staff who wish to publish information on social media networks on behalf of the council. The following is an extract; users must read the full guidance.

All social media sites that conduct business on behalf of the council must be authorised by Corporate Communications. The exception is Education and Families staff in schools who may create a social media page or blog as part of a learning and teaching environment or as a communication tool; this should be arranged in conjunction with ICT.

Employees are prohibited from setting up a site and using it for council business, unless authorisation has been provided by Corporate Communications.

Corporate Communications will delete posts or comments when these contain inappropriate content. This includes, but is not restricted to, the following.

- Comments that are politically motivated, insulting, obscene or racist.
- Material that perpetuates or promotes discrimination of protected characteristics. These characteristics can include but are not limited to, race, gender, disability, age, sexual orientation, religion or belief, pregnancy and maternity, marriage or civil partnership or gender reassignment.
- Sexual content or links to sexual content.
- Solicitation of commerce.
- Illegal conduct or encouragement/support of illegal activities.
- Information that compromises or may compromise the safety or security of the public or public systems.
- Content that violates the legal ownership interests of any other party.

Publishers may respond to comments on social media sites where they feel knowledgeable and confident to do so, particularly where someone is looking for help, having a problem with a service we provide, or are incorrect. Where they are unable to respond to such posts, they should contact their manager or inform the relevant service.

Where a mistake is made in a posting, it should be publicly corrected at the earliest opportunity.

Where an issue is potentially damaging to the reputation of the council, Corporate Communications should be informed. When representing the council on social media, employees must not comment on government policies and practices. They should also not comment on politically controversial issues. This also applies to other activity such as surveys, service promotion and discussions.

This guidance always applies, but additional guidance will be supplied, and should be read in conjunction with this policy, during any pre-election period, or in the lead up to a Referendum. The pre-election period is the term used to describe the period between the time an election is announced and the date the election is held. If there is any doubt about whether an action is appropriate, users should not take it and seek guidance from their manager.

The council's Yammer social media platform can be used by all staff for internal informal communication – Yammer Guidance.

Note that other social media apps such as WhatsApp, Messenger etc. aren't currently supported on council devices, and are not an approved form of communicating business information on personal devices.

Inappropriate Use of ICT

Examples of inappropriate use include the following, although the list is not exhaustive.

- Downloading or distributing pirated software or data
- Intentionally circulating any computer virus
- Disabling any computer system or network
- Accessing and/or communicating information that is confidential to the council, unless authorised to do so
- Sending or forwarding any message (inside or outside the organisation) that could constitute bullying or harassment or be interpreted as offensive
- Sharing images that are inappropriate or links to inappropriate content.
- Excessive use of systems for non-work-related activity

Suspected inappropriate use will be investigated under the council's Discipline Policy.

Employees must take particular care to understand the copyright trademark to ensure their use of the internet does not inadvertently violate any laws which might be enforceable against the council.

E-mail Operating Principles

Personal or confidential information should not be sent to personal email accounts as this is not a secure route. Email auto-forwarding to non-council addresses should not be used. Employees who require access to email and other systems should use the council's remote access systems for this purpose.

Users will:

- Only use appropriate language in messages, emails, faxes and recordings. Threatening, derogatory, abusive, indecent, obscene, racist, sexist or otherwise offensive content will not be tolerated
- Not engage in mass transmission of unsolicited emails (SPAM).
- Not alter the content of a third party's message when forwarding it unless authorised.
- Not try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures).
- Be vigilant to phishing emails and know how to spot and report suspicious emails.
- Employees and contractors must not use their council email address for personal use. Only use your council mail address for business related activities and linked organisational activity (e.g. NLC discount schemes, Civil Service Jobs, Trade Union activity and other officially provided internet links).

Collaboration Tools

Microsoft Teams is the recommended tool for communication and collaboration, combining workplace chat, video meetings, file storage, and application integration. However, the main collaboration tool for teaching staff is Glow which includes Teams and other O365 services for Education.

Use of collaboration tools must adhere to the following principles (not applicable to Education staff, who will comply with Glow usage guidance).

- All Teams require a minimum of two owners, to maintain business continuity. These owners are responsible for managing membership and content.
- Access is from a managed corporate Windows 10 device or a managed mobile device only. Other devices, such as 'Bring Your Own Devices' (BYOD) are not supported.
- Collaboration will be restricted to internal use only, unless a specific business requirement is identified and external sharing approved.
- Guest access will be permitted where there is a valid business purpose.
- Chat functionality is for business related purposes only, unless agreed or approved otherwise.
- Owners are responsible for creating channels.
- Private Channels within Teams are not allowed although this may be reviewed if there is a justified business case.
- New Teams can only be created by ICT administrators, a request should be submitted to the ICT Service Desk.
- Team names must be relevant to the service or piece of work that is being carried out. For example, a Team cannot be called 'HR' if it is not owned by HR.
- Personal/copyright material, such as pictures, music or videos should not be stored in Teams.
- Data in a Team will be retained and disposed of in line with the council's retention schedule.
- Teams that are no longer in use, or have not been used for a period, will be deleted after six months in line with the disposition process.
- Other tools such as Attend Anywhere, Skype for Business, Webex, etc may be used to join collaborative sessions; these will be assessed by ICT as required.
- Cisco Webex is available for a limited period on a small scale for collaboration use, this should adhere to the same standards detailed above
- Education and Families staff must also comply with the principles outlined in the Digital Learning and Teaching Approaches Policy and usage Guidance issued for schools staff.

Whilst Bring Your Own Device (BYOD) is not presently supported for access to systems it is under regular review.

Personal use of Council Technology

Use of council technology and systems such as internet, telephone and email are primarily for business use. However, the council operates a framework of openness and trust and recognises that in certain circumstances, particularly where there is a need to communicate urgently, it may be appropriate for employees to use council facilities, for example to send personal messages externally or receive them from an outside source.

Limited personal use of internet facilities is permitted during breaks provided that the material accessed is appropriate and is not potentially offensive. The use of the internet for personal transactions only, such as booking reservations or tickets or the purchase of any goods or services for personal use, is permitted. Employees should regard this facility as a privilege that should not be abused.

Users will:

- Understand that they are personally accountable for what they do online and with council technology.

- Note that personal use of ICT resources is permitted in an employee's own time when not on official duty or 'flexed on' as per the Flexible Working Hours Policy.
- Ensure that any personal information stored is appropriate i.e. legal, appropriate and compliant with this policy.
- Understand that the ability to store personal information on council-owned devices and systems is a privilege and the council has a right to require the data is removed should this data interfere with business activity or use.

In consideration of colleagues, while in a shared workplace, mobile phones or other personal devices should be set on discreet or low volume mode. Services, individual offices, or specific work environments may have special sets of standards that will apply.

There are situations where mobile phone use may be banned, especially in customer facing roles such as teaching, in customer services offices, and social services settings. In certain work situations, the use of a mobile phone is not permitted as this may affect the health and safety of yourself/colleagues/public and you should ensure that you are aware of service rules.

Outside of Work

The Employee Code of Conduct describes employees' rights and responsibilities to make public statements about the council as a citizen. These rights and responsibilities apply both to traditional and new media including social networking sites. Be conscious that any content placed on them may be seen by people other than the intended audience and must be considered public.

Working from Home

When working from home, employees should be as vigilant as they would be in the office. Care should be taken to lock equipment when not in use, ensure conversations cannot be overheard and council information is stored securely. See home working guidance.

6. Monitoring

Access to council information processing systems and facilities is provided for business use. While sensible personal use is permitted, misuse or prohibited use shall be dealt with under the disciplinary process.

A range of monitoring is undertaken to ensure information processing facilities are operating efficiently and effectively. Information entering, leaving or stored on information processing facilities, including council email, is monitored. The monitoring undertaken is not generally focused on specific individuals, however personal data may be accessed as part of the procedure.

By logging in to any council information processing system or facility a user is deemed to consent to the council's monitoring procedures. Monitoring is undertaken to:

- comply with regulatory and statutory obligations
- maintain the effectiveness of information processing systems
- prevent or detect unauthorised use or other threats to information processing systems
- prevent or detect criminal activities
- ensure compliance with council policies and procedures, and
- review usage.

To ensure information processing systems are not open to abuse, the council reserves the right to monitor individual employee's usage. This level of monitoring will be fair and proportionate and will be appropriately authorised.

7. Privacy

This policy aims to strike a balance between respect for an individual's privacy while enabling the monitoring and scanning necessary to fulfil legal obligations and business needs.

Individuals' privacy will be respected in accordance with the Human Rights Act 1998 and the Data Protection Act 2018. The council will act in accordance with its obligations under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Regulation of Investigatory Powers Act 2000 (RIPA).

Monitoring differentiates between:

- Usage logging - collecting data, generally from system log files about how and when a user id accessed and used information processing systems
- Content inspection - viewing information held in business or personal files, email etc. or viewing information on screen. Content inspection will take place only if properly authorised and if the usage record alone is not sufficient.

Usage Logging

Usage logging ensures and improves service performance and helps identify and investigate potential prohibited use or misuse.

- Typical data logged is noted below
- No content is logged, only information about the activity
- Access to logging information is restricted and controlled

Content Inspection

Inspection will only be undertaken for legitimate reasons which may include the following.

- Where we believe that a breach of the policy is occurring or has occurred
- To comply with the request of law enforcement officers
- To comply with legal obligations
- To prevent or detect contravention of criminal or civil law
- Where we believe that a breach of an individual's employment contract is occurring or has occurred

Content inspection may involve viewing information held in:

- Business and or personal files and documents
- Business and or personal email messages or any other ICT based communication
- Business and or personal information displayed on a screen
- Emails that have not yet been opened or received by the intended recipient.

Requests to inspect content must be formally approved at Head of Service level or above.

Managers will normally seek authorisation from a Head of Service. However, where the request involves a Head of Service, authorisation should be sought from an Executive

Director, and where the request involves an Executive Director or Elected Member, authorisation should be sought from the Chief Executive.

Where authorisation is granted, the authorising officer must advise the Chief Executive and the individual concerned as appropriate.

The individual concerned should normally be informed of any inspection in advance and again on completion. However, in certain circumstances it may be necessary to obtain access without informing the individual, such as where there is reason to believe that to do so would prejudice an investigation.

8. Advice or guidance

Guidance on the application of the policy can be sought from:

- Line managers for guidance on interpretation
- ICT Service Desk for guidance on good practice
- Information Risk Manager for policy guidance and general advice

9. Governance

The ICT Acceptable Use Policy will be monitored and reported through the Transformation and Digitilisation Committee.

Equalities and Fairer Scotland

The principle of equality of opportunity is central to all aspects of Digital and ICT policies and plans. An Impact Assessment was carried out to ensure adherence to our corporate commitment to the Single Equality Scheme.

Risk Management

This policy is one of the control factors for the Information Security and Governance corporate risk.factors for the Information Security and Governance corporate risk.

HR and Legislative

The ICT Acceptable Use Policy complies with all relevant legislative requirements.