

Acceptable Use of IT Policy

Version 4.1, 21 February 2024

This is a controlled document. The digital PDF file published on InsideNL is the control copy.

- Always access this document from the [control location](#).
- When you open this document, your device may automatically download it. If it does, you should still open it from the control location in future.
- You can print this document, but a printed copy isn't the control copy.
- Don't save any digital copies of this document anywhere. This includes your device, USB flash drives, network drives, OneDrive, Teams/SharePoint, or any other digital storage device, system, service, or location.

**LIVE
LEARN
WORK
INVEST
VISIT**

Document control

Title	Acceptable Use of IT Policy		
Governance group	Policy and Strategy Committee		
Owner	Katrina Hassell, Senior Information Risk Officer	Contact	hassellk@northlan.gov.uk
Author	Julie Irwine, Information Compliance Officer	Contact	irwinej@northlan.gov.uk

Revision history

Version	Originator	Review start date	Revision description and record of change
4.0	Julie Irwine	16 February 2022	Bi-annual review and plain English changes.
3.2	Rob Leitch	June 2020	Updated link to home working guidance on MyNL.

Document approvals

Version	Governance group	Date approved	Date approval to be requested (if document still in draft)
4.0	Finance and Resources Committee	22 November 2023	
3.0	Finance and Resources Committee	03 June 2021	
2.0	Finance and Resources Committee	11 June 2020	
1.3	Policy and Resources Committee	21 June 2017	
1.2	Policy and Resources Committee	16 September 2014	
1.1	Policy and Resources Committee	14 March 2013	

Consultation record (for most recent update)

Consultation status	Stakeholders consulted between 02 March 2023 and 10 May 2023.	
Stakeholders consulted and dates	Business and Digital Management Team	21 March 2023
	Corporate Communications	02 March 2023
	Data Governance Board	29 March 2023
	Data Management Team	15 March 2023
	JNC for Teaching Staff	30 March 2023
	Joint Trade Unions	30 March 2023
	People Resources	15 March 2023
	Technical Design Authority	21 March 2023

Strategic alignment

Plan for North Lanarkshire

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.

Digital and IT Strategy

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 IT Policy is one of these. It supports the strategy by providing a safe framework for using IT assets without exposing the council or our IT users to risks.

Next review date

Review Date	November 2025
--------------------	---------------

Contents

1. Introduction	1
2. Purpose	1
3. Scope and exclusions.....	1
4. Governance.....	2
5. Policy compliance	2
6. Acceptable use of IT assets.....	3
6.1. IT authentication (password) and secure access	3
6.2. Protecting digital information.....	3
6.3. Managing digital information	4
6.4. Appropriate use of IT assets	4
6.5. Using email.....	5
6.6. Using collaboration platforms	6
6.7. Using social media.....	6
6.8. Personal use of council IT assets.....	6
6.9. Using personal devices, software and cloud accounts.....	7
6.10. Reporting information security incidents.....	8
7. Monitoring	8
7.1. Monitoring activities and privacy	8
7.2. Types of monitoring	9
7.3. Identifying and investigating potential misuse	9
8. Product set.....	10

A note about links to documents stored on InsideNL

This document has links throughout to other documents, websites and IT systems, as listed in the product set. Some documents are stored on our intranet, InsideNL. If you don't have access to InsideNL but want to view a document stored there, ask your line manager to arrange for a copy to be sent to you.

A note about plain English

This document follows [plain English guidance](#), in line with our corporate commitment to clear communications. In particular, it uses the following terms.

- 'We', 'us' and 'our' when referring to the council (as an organisation), our collective responsibilities (as authorised users of council IT assets), and when discussing specific activities.
- 'You' and 'your' when referring to the individual responsibilities and actions of authorised users of council IT assets.

1. Introduction

We use information technology (IT) to deliver our services, carry out our statutory duties, and support our internal business functions. It's critical in helping us work flexibly and efficiently. This policy informs our IT users on how to use IT assets appropriately.

We use the following three types of IT assets – see the [Acceptable Use of IT Guidance](#) for examples of each.

1. **Computing devices** (both business and personal) we use in council facilities and remotely to access information and do our jobs.
2. **IT systems and services**, both hosted within our own network and cloud-based, that we use to process and store information and deliver services.
3. **Network infrastructure and services** we use to access, store, manage and protect our systems.

The council owns all information stored on council assets.

2. Purpose

This Acceptable Use of IT Policy provides a safe framework for using IT assets without exposing the council or our IT users to risks. It is a control factor for the Information Security and Governance corporate risk and aligns with the following.

- [Digital and IT Strategy](#) – this brings together separate but related plans and policies – including this one – that contribute to our digital vision.
- Information governance policies – [Data Protection](#), [Information Security](#), [Payment Card Data Security](#), [Records and Information Management](#) – that keep our IT assets safe and operational, and maintain the confidentiality, integrity and availability of our information.
- Codes of conduct that set out mandatory standards for [Councillors](#) and [Employees](#).
- Related [legislation](#).

3. Scope and exclusions

In scope: This policy applies to our employees, councillors, contractors, consultants, third party service providers, temporary agency staff, modern apprentices, students, volunteers, and anyone else authorised to access or use our IT assets.

Exclusions: There are separate policies for the [schools' network](#) and [public use of IT resources and the internet in libraries](#).

4. Governance

The Finance and Resources Committee has approval authority for, and oversight of, this policy. The Data Management Team then the Data Governance Board – as key stakeholders – oversee its review and consider its contents before referring it on for approval. The Chief Officer of Business and Digital – as the council’s Senior Information Risk Owner – is accountable for its governance.

The Information Security and Risk team is responsible for the following activities.

1. Produce, publish and promote this policy.
 - a. Write it in a way that’s easy to read and understand.
 - b. Consult with relevant stakeholders on its content and implications.
 - c. Make sure all users can access it.
2. Give guidance on how to apply and comply with this policy through standards, procedures and guidance notes – see [product set](#) for list and links.
3. Review and report on this policy.
 - a. Review every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, an audit action.
 - b. Report to management teams, governance and working groups, committees and scrutiny panels.

5. Policy compliance

By using our IT assets, every user is agreeing to comply with this policy, and all policies, standards, procedures, and guidance it references.

This includes following the [acceptable use principles](#) below, understanding that we [monitor usage](#) of all our IT assets, and consenting to this monitoring.

Due to the importance of this policy and as a consistent reminder, our computers and laptops display an Acceptable Use of IT Policy statement that users must accept before they can log in to their device.

We only use council managed devices to access council systems
and conduct council business – subject to [limited exceptions](#).

We [investigate any suspected breach of this policy](#), under the [Discipline Policy](#) and any other relevant policies.

We refer any suspected unlawful acts to the appropriate authorities. This includes the police, and professional and regulatory bodies.

6. Acceptable use of IT assets

All users of our IT assets must:

- comply with this policy, in line with the acceptable use of IT principles below; and
- fulfil their role in assuring the security and integrity of council information and IT assets, as outlined in the user responsibilities below.

Acceptable use of IT principles

1. [IT authentication \(password\) and secure access](#)
2. [Protecting digital information](#)
3. [Managing digital information](#)
4. [Appropriate use of IT assets](#)
5. [Using email](#)
6. [Using collaboration platforms](#)
7. [Using social media](#)
8. [Personal use of council IT assets](#)
9. [Using personal devices, software and cloud accounts](#)
10. [Reporting information security incidents](#)

The user responsibilities for the acceptable use of IT assets – summarised below and detailed in the [Acceptable Use of IT Guidance](#) – instruct users on how to confidently and securely access and use council devices and information. The Information Security and Risk team can help with questions about this policy and associated guidance:

- ✉ anyone can send an [email](#) enquiry; and
- 🔗 employees with access to Viva Engage (also known as Yammer) can post a question on the [Information Security and Risk](#) community page.

6.1. IT authentication (password) and secure access

User responsibilities for IT authentication (password) and secure access


1. Pick strong, unique passwords.
2. Secure your passwords and other secret information.
3. Never share credentials.
4. Pick memorable information and security question answers that aren't easily guessable, if a system uses any of these as a secondary authenticator.
5. For full details, read the [IT Authentication \(Password\) and Secure Access User Guidance](#).

6.2. Protecting digital information

User responsibilities for protecting digital information

1. Be vigilant always, wherever you are working – in the workplace, at home and other remote locations, and in public spaces.
2. Keep information safe.
 - a. Use a headset wherever possible to limit what others can hear.

User responsibilities for protecting digital information

- b. Never work on sensitive information where unauthorised people can see or hear it.
- c. Only print paper copies if there's a business reason for not sharing digitally.
- d. Only use dictation and read aloud assistive technology in a secure location.
- e. Don't access information unless you have a valid business reason to do so.
- f. Follow procedures for [data protection subject access](#) and [freedom of information](#) requests.
- g. Only give out information when authorised, it's appropriate to do so, and the recipient's identity is verified, where needed.
- h. Lock your device whenever you leave it for a short while but are still using it:
Windows logo key  + L.
- i. Log out of your device and close it down when you're no longer using it.

6.3. Managing digital information

User responsibilities for managing digital information

1. Make sure all information you create, use, process, store, share and dispose of is in line with business need and complies with our [information governance policies](#).
2. Follow the rules set out in the [Information Classification and Handling Standard](#) and [Information Classification and Handling Guidance](#).
3. See the [Records Retention Schedule](#) to decide how long to keep information and how to dispose of it.
4. Know where to store and publish digital information. This includes shared and personal storage areas, network drives, business systems, other file sharing platforms, internal communications platforms, and our websites.

6.4. Appropriate use of IT assets

User responsibilities for the appropriate use of IT assets

1. Technical and systems administrators must have prior authorisation to give access to the systems and services they manage, in line with [access control](#) and [code of connection](#) procedures.
2. Use access rights appropriately – in line with job roles and responsibilities.
3. Stay safe online when using search engines, visiting websites and other internet-based services. The [Get Safe Online](#) website – a [Cyber Scotland](#) partner – provides advice.
4. Never create, store, view, download, or share (links and attachments) inappropriate content that do any of the following.
 - a. Use unacceptable language.
 - b. Insult, target or [discriminate](#) against people with protected characteristics.
 - c. Could be interpreted as politically motivated, bullying, abusive, offensive, or illegal.
 - d. Contain images, videos or written materials that are sexually explicit or exploitative, or promote discrimination, hate, violence, extremism or terrorism.

User responsibilities for the appropriate use of IT assets

- e. Send or post unsolicited or fraudulent messages. This includes spam, phishing and assumed identity.
 - f. Infringe [copyright](#) online, while acting on behalf of the council.
 - g. Operate or promote any private businesses or commercial ventures.
5. If a user accidentally breaks any of these rules, they must tell their manager straight away, and – if necessary – log an incident on the [IT self-service portal](#).
6. Understand that we [investigate](#) all suspected inappropriate activity.

6.5. Using email

User responsibilities for using email

1. Never use email or any other digital messaging facility to send or share [inappropriate content or communications](#), as described in section 6.4 above.
2. Users must use the council email system for work-related activities.
 - a. Use **individual council email accounts** for work and organisational activities.
 - b. Use **shared email accounts** – where appropriate – to collectively manage team-level communications.
3. Users must not do any of the following.
 - a. Send work related email or information to their own personal email address.
 - b. Send work related email or information to any other personal or external email addresses – except when in line with points 2f and 2g of the [protecting digital information](#) guidance in section 6.2 above.
 - c. Use a council email address to send or receive personal messages - except in [emergencies](#) as detailed in section 6.8 below.

Note: Our email filtering software may quarantine personal email messages as potential phishing. We will not release them.
 - d. Use a non-council email address to send or receive work related messages – subject to authorised exceptions relating to third party users and IT system notifications.
 - e. Edit the content of a third party's message, unless authorised to do so.
4. Be vigilant! Malicious email – including scam and phishing attempts – is our biggest IT security threat. Follow [email security guidance](#) on spotting and reporting suspicious email.

Users must phone the IT Service Desk straight away if they have opened an attachment or clicked on a link in a suspicious email.

See [reporting information security incidents](#) in section 6.10 below for more details.
5. Read the [Records Retention Schedule](#) for information on retaining and disposing of email and [Information Classification and Handling Guidance](#) for rules on sharing email messages.

6.6. Using collaboration platforms

User responsibilities for using collaboration platforms

1. We use Microsoft Teams and SharePoint to communicate, collaborate, chat, meet, share and store files, and access other IT products.
2. Only access our collaboration platforms from council devices. Don't use [personal devices](#).
3. Don't store personal files and media or copyrighted materials on [our storage facilities](#).
4. Users can join collaborative sessions hosted by other organisations on other approved browser-based platforms.
5. Read the [Information Classification and Handling Guidance](#) for information on storing and posting content on collaboration platforms, and the [Records Retention Schedule](#) for guidance on retaining and disposing of it.

6.7. Using social media

User responsibilities for using social media

1. Corporate Communications is responsible for our [Corporate Communications Strategy](#) and the supporting [Guidance for using social media for work purposes](#).
2. The council owns all social media accounts that communicate and conduct business on its behalf.
3. The Corporate Communications team has authority over every council social media account – as detailed in and subject to the exceptions in the [social media guidance note](#).
4. Owners and publishers of council social media accounts must only use council devices, follow the [social media guidance](#), and never publish or share [inappropriate content or communications](#) as described in section 6.4 above.
5. All users with access to Viva Engage (also known as Yammer) – our private, internal social network – can post informal communications and comments. See [user guidance](#).
6. See the [Information Classification and Handling Guidance](#) for rules on posting information on our social networking sites.
7. Read the [Employee Code of Conduct](#) for guidance on personal use of social media and your rights and responsibilities relating to expressing personal views about the council, maintaining confidentiality, and professional and ethical conduct.

6.8. Personal use of council IT assets

User responsibilities for personal use of council IT assets

1. Council IT assets are primarily for business use, but we do allow [appropriate](#) personal use. For example:
 - a. using council devices and systems to send or receive personal email messages or phone calls in an emergency, and
 - b. general web browsing during breaks and lunch.

User responsibilities for personal use of council IT assets

2. Users who choose to make use of this privilege, must follow these rules.
 - a. [Comply with all relevant council policies](#), including this one.
 - b. Don't use council IT assets for private business or commercial ventures.
 - c. Don't do it during work time.
 - d. It must not interfere with normal business or negatively impact productivity.
 - e. Don't store personal files on any of [our storage facilities](#).
 - f. Understand that:
 - we own all information stored on council IT assets – both business and personal;
 - all personal use is subject to the same [monitoring activities](#) as business use;
 - users are personally accountable for what they do with council IT assets, including online activity; and
 - if a user abuses this privilege, we reserve the right to withdraw it, and will investigate their activity if we suspect [potential misuse](#).

6.9. Using personal devices, software and cloud accounts

User responsibilities for using personal devices, software and cloud accounts

1. We don't allow personal devices access to the council network, or any systems or services hosted there. There are no exceptions to this, and users must not attempt it.
2. We also don't allow personal devices access to our cloud hosted systems and services, including [collaboration platforms](#), as detailed in section 6.6 above. However, there are exceptions to this, as listed below. These are the only exceptions. Users must not attempt to access any of our other cloud hosted systems and services using personal devices.
 - a. iTrent – staff can only manage their own mySelf personal records.
 - b. Viva Engage (also known as Yammer) – to allow staff to read and contribute to conversations.
 - c. Public facing websites – users can view content on council websites.
 - d. Social media platforms – viewing content on platforms where we have a presence. [Users must not use a personal device when using social media for work purposes.](#)
 - e. Microsoft Authenticator – a free app users install on their personal device to authenticate onto the council network and M365 when working remotely.
3. Users must not use software, systems or services they have personally licensed, purchased, registered an account with, or subscribed to, for work purposes. This includes software on personal devices, and cloud-hosted systems and services accessed from any device.
4. We generally allow personal mobile devices in shared workplaces.
 - a. For courtesy and privacy reasons, users should set sound mode to low volume and or vibrate and take calls where they won't be overheard.

User responsibilities for using personal devices, software and cloud accounts

- b. In some work settings users may not be allowed to use personal mobile devices, have them visible or even on their person for privacy or health and safety reasons. Line managers can give more guidance on this.

6.10. Reporting information security incidents

User responsibilities for reporting information security incidents

1. We must report information security incidents straight away to the Service Desk and or Data Protection Team and to line managers if:
 - a. someone has logged on to a device or system using another person's details;
 - b. a device is lost or stolen; and or
 - c. there may be a system or data breach.
2. There may be other reporting requirements, depending on the type of incident.
3. For full details see the [Information Security Incident Management Procedure](#) and the [Data Protection Breach and Incident Management Protocol](#).

7. Monitoring

7.1. Monitoring activities and privacy

We carry out a range monitoring activities of our IT assets for compliance, security, operational, performance, and maintenance purposes.

A note on respecting individual privacy.

This policy aims to strike a balance between the following.

1. Respect for an individual's privacy in accordance with the
 - [Data Protection Act 2018](#), and
 - [Human Rights Act 1998](#).
2. Our monitoring and scanning obligations under the
 - [Regulation of Investigatory Powers Act 2000](#), and
 - [Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)

Users can't presume privacy when using council IT assets for business or personal reasons. By using our IT assets and agreeing to [comply with this policy](#), they are consenting to our monitoring procedures. We:

- collect and record usage data to make sure our IT assets work correctly and securely;
- monitor information entering, leaving, or stored on our IT assets; and
- don't routinely monitor individuals but may access personal information as part of our monitoring activities.

7.2. Types of monitoring

There are two types of monitoring.

1. **Usage logging:** This is a standard data collection activity data – generally in system event logs. It does not log content, only information about user activity. We restrict and control access to logging information.
2. **Content inspection:** That is, viewing the actual digital data, information and records within files and IT systems – both business and personal – that users create, modify, access, view and receive.

7.3. Identifying and investigating potential misuse

We reserve the right to monitor individual usage – under strict controls – to help identify and investigate potential prohibited use or misuse in breach of this policy and or [codes of conduct](#).

Managers must have formal approval before they can request access to this information. Once approved, they must use the [IT self-service portal](#) to make their request.

Formal approval authority

- A Chief Officer must approve requests for employees within their service.
- The Depute Chief Executive must approve requests for Chief Officers in Adult Health and Social Care, Education and Families, and Enterprise and Communities.
- The Chief Executive must approve requests for Chief Executive’s Chief Officers, Depute Chief Executive or Councillors.
- The Leader of the Council must approve request for the Chief Executive.

- **Level 1 investigation: Inspecting user logs** – to determine if there has been a breach; and or we have cause to investigate further.
- **Level 2 investigation: Inspecting content** – where there is a need to investigate more thoroughly than inspecting user logs alone. For example, where we believe there is or has been a breach of this policy, to comply with the request of law enforcement officers, or where we believe an employee is or has been in breach of their employment contract.

Where an officer authorises a content inspection request, they must advise the following people before it starts and when it’s finished.

1. The Chief Executive or the Leader of the Council – as per the formal approval authority.
2. The individual concerned. However, there may be situations where we can’t inform them. For example, where there is reason to believe that this would prejudice or compromise an investigation.

See the [Discipline Policy and Discipline Policy Guidance Note](#) for more information.

8. Product set

The table below lists documents in the acceptable use of IT product set and other related products. This may include links to other file types, websites and IT systems.

- Those listed under **policies, standards, procedures, and guidance** are the responsibility of the Information Security and Risk team.
- Those listed under **related products and legislation, regulations, and government guidance** are the responsibility of other teams, services or agencies.

Product type	Product
Policies	<ul style="list-style-type: none"> ▪ Information Security Policy ▪ Payment Card Data Security Policy
Standards	<ul style="list-style-type: none"> ▪ Information Classification and Handling Standard
Procedures	<ul style="list-style-type: none"> ▪ Access control procedures ▪ Code of connection procedures ▪ Information Security Incident Management Procedure
Guidance	<ul style="list-style-type: none"> ▪ Acceptable Use of IT Guidance ▪ Email security guidance ▪ IT Authentication (Password) and Secure Access User Guidance ▪ Information Classification and Handling Guidance ▪ Information Security and Risk on Viva Engage (also known as Yammer)
Related products	<ul style="list-style-type: none"> ▪ Corporate Communication Strategy ▪ Cyber Scotland ▪ Data Protection Breach and Incident Management Protocol ▪ Data Protection Policy ▪ Data protection subject access requests ▪ Digital and IT Strategy ▪ Discipline Policy and Discipline Policy Guidance Note ▪ Employee Code of Conduct ▪ Freedom of information requests ▪ Get Safe Online ▪ Guidance on the use of social media for work purposes ▪ IT self-service portal ▪ Public use of IT resources and the internet in libraries ▪ Records and Information Management Policy ▪ Records Retention Schedule ▪ Schools' policy documents on Glow

Product type	Product
Legislation, regulations, and government guidance	<ul style="list-style-type: none"> ▪ <u>Computer Misuse Act 1990</u> ▪ <u>Copyright information: GOV.UK</u> ▪ <u>Councillors' Code of Conduct</u> ▪ <u>Discrimination: your rights: GOV.UK</u> ▪ <u>Data Protection Act 2018</u> ▪ <u>Ethical Standards in Public Life etc. (Scotland) Act 2000</u> ▪ <u>Freedom of Information (Scotland) Act 2002</u> ▪ <u>Human Rights Act 1998</u> ▪ <u>Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping purposes) Regulations 2018</u> ▪ <u>Public Records (Scotland) Act 2011</u> ▪ <u>Regulation of Investigatory Powers Act 2000</u> ▪ <u>Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000</u> ▪ <u>The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020</u>