



Information Security and Risk Acceptable Use of IT Guidance

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

Control details

Title:	Acceptable Use of IT Guidance
Author:	Julie Irwine, Information Compliance Officer
Owner:	Rob Leitch, Information Risk Manager
Subject:	<p>Acceptable Use of IT Guidance, in support of the Acceptable Use of IT Policy.</p> <p>This guidances helps our IT users understand their responsibilities for the acceptable use of IT assets, and explains the monitoring activities we use to protect our IT assets.</p>
Classification:	OFFICIAL
Control location:	<p>InsideNL > Documents > Information governance > Information security and risk > Acceptable use of IT</p> <p>Save this link to your browser favourites for quick and easy access.</p>
Published version:	Version 4.1
Published date:	21 February 2024
Review date:	Two years from date of last review.
Retention and disposal:	<p>Retention period: Two years after date superceded</p> <p>Disposal action: Destroy</p>
Distribution and communication:	<p>This document is available to all users and the control PDF is published on InsideNL. It's primary audience is everyone who uses, administers or manages council information. We inform staff about it through induction and training, email, InsideNL and Viva Engage (alsk known as Yammer). This includes</p> <ul style="list-style-type: none"> ▪ reporting on newly published versions, ▪ awareness campaigns, and ▪ as a response to any relevant security incidents.

Amendment record

Version	Amendment details	Amended by and date
4.1	Clarifications regarding using work email and personal devices. Examples included.	Julie Irwine 21 February 2024
4.0	Transferred to new template, plain English revisions, amendments to reflect our new digital environment, and detailed guidance, in line with version 4.0 of the Acceptable Use of IT Policy.	Julie Irwine 13 February 2024
3.0	Updates to align with version 3.0 of the Acceptable Use of IT Policy.	Rob Leitch and Charles Muir 08 June 2021

Contents

1	Introduction	1
2	Purpose	1
3	Compliance	1
4	Acceptable use of IT assets	2
4.1	IT authentication (password) and secure access	3
4.2	Protecting digital information	3
4.3	Managing digital information	4
4.4	Appropriate use of IT assets	5
4.5	Using email	7
4.6	Using collaboration platforms	8
4.7	Using social media	9
4.8	Personal use of council IT assets	10
4.9	Using personal devices, software and cloud accounts	10
4.10	Reporting information security incidents	11
5	Monitoring	12
5.1	Monitoring activities and privacy	12
5.2	Types of monitoring	13
5.3	Identifying and investigating potential misuse	13
6	Product set	14

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. The [Acceptable Use of IT Policy](#) aligns with the [Digital and IT Strategy](#) and informs our IT users on how to use IT assets appropriately. This guidance supports that policy and explains:

1. user responsibilities for the acceptable use of IT assets; and
2. the monitoring and investigation activities we use to protect our IT assets.

The council owns all information stored on our IT assets.

2 Purpose

This document gives guidance on how to **use IT assets without exposing the council or yourself – as an IT user – to risks**. Our IT assets include computing devices, IT systems and services, and network infrastructure and services – see definitions below.

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

Defining IT assets

We use the following three types of IT assets.

1. **Computing devices** – both business and personal – we use in council facilities and remotely to access information and do our jobs. This includes laptops, mobile phones, equipment aids, and multi-functional devices that print, scan and photocopy.
2. **IT systems and services** – both hosted within our own network and cloud-based – we use to process and store information and deliver services. This includes business systems and applications, assistive technology, office software, databases, websites, and apps.
3. **Network infrastructure and services** we use to access, store, manage and protect our systems. This includes hardware and software – both within our own network and through cloud managed services – including routers, switches, gateways, firewalls, servers, and monitoring and management tools.

3 Compliance

By using our IT assets, you are agreeing to comply with the [Acceptable Use of IT Policy](#), and all [policies, standards, procedures and guidance](#) it references. This includes:

- following the acceptable use principles below;
- agreeing to the Acceptable Use of IT Policy statement below, that displays on your computer or laptop before you can log in to your device;

Acceptable Use of IT Policy

All North Lanarkshire Council Information Technology (IT) users **must** comply with our Acceptable Use of IT Policy. By logging into this device or using any of our IT assets – including other devices, IT systems and services, and network infrastructure – you are agreeing to comply with this policy. To accept this, click the OK button below to log on as normal.

- **only using council managed devices to access council systems and conduct council business** – subject to [limited exceptions](#); and
- understanding that we
 - monitor usage of all our IT assets,
 - [investigate any suspected breach of this policy](#), under the [Discipline Policy](#) and any other relevant policies, and
 - refer any suspected unlawful acts to the appropriate authorities – including the police, and professional and regulatory bodies.

4 Acceptable use of IT assets

As a user of our IT assets, you **must**:



- comply with the [Acceptable Use of IT Policy](#) – in line with the acceptable use of IT principles below; and
- fulfil your role in assuring the security and integrity of council information and IT assets, as defined 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** detailed below tells you how to access and use council devices and information confidently and securely.

The Information Security and Risk team can help with questions about the Acceptable Use of IT Policy and this guidance:

-  anyone can [email](#) their enquiry; and
-  employees with access to Viva Engage (also known as Yammer) can post questions on our [Information Security and Risk](#) community page.

4.1 IT authentication (password) and secure access

User responsibilities for IT authentication (password) and secure access


1. Pick strong, unique passwords. You must have a separate and distinct password for each system you access. Never share passwords between business and personal accounts.
2. Secure your passwords and other secret information. Keep them safe. Never write them down. Use browser and system 'remember me' functionality on your council device but not on any public or personal devices.
3. Never share credentials.
 - Never share your passwords or secret information with anyone.
 - Never ask or compel anyone into give you their password or secret information.
 - Never log into a system using someone else's 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](#).

4.2 Protecting digital information

User responsibilities for protecting digital information

1. Be vigilant always, wherever you are working – in the workplace, [at home](#) or another remote location, or in public spaces. You – and the council – have a legal responsibility to protect our information.
2. Do the following to help keep information safe.
 - a. Use a headset wherever possible to limit what others can hear – for phone calls, online meetings and read-aloud assistive technology.
 - b. Never work on sensitive information where unauthorised people can see it or hear you discussing it.
 - c. Only print paper copies of information if there's a business reason for not sharing digitally, in line with [information handling guidance](#).
 - d. When using assistive technology that supports dictation and read aloud functionality, only use it in a secure location.
 - e. **Don't** access information unless you have a valid business reason to do so.
 - f. Follow the procedures for handling [data protection subject access](#) and [freedom of information](#) requests.
 - g. Only give out information when:
 - you are authorised to do so;
 - it's appropriate to give it to the person you want to send it to; and
 - where needed, you can verify the recipient's identity.

User responsibilities for protecting digital information

- h. Lock your device whenever you leave it for a short while but are still using it. On your keyboard, either use
 - Windows logo key  + L, or
 - Ctrl + Alt + Delete then click on Lock.
- i. Log out of your device and close it down when you're no longer using it.

4.3 Managing digital information

User responsibilities for managing digital information

1. Make sure all information you create, use, process store, share and dispose of it in line with business need and complies with our information governance policies.
 - [Data Protection](#)
 - [Information Security](#)
 - [Payment Card Data Security](#)
 - [Records and Information Management](#)
2. Follow the rules set out in the [Information Classification and Handling Standard](#) and [Information Classification and Handling Guidance](#), covering:
 - processing, copying, sharing, publishing, and posting information;
 - storing, disposing of, and archiving information; and
 - carrying digital information on a computing device.
3. See the [Records Retention Schedule](#) to help you decide
 - how long to keep information, and
 - whether to dispose of, archive or permanently preserve it.
4. Know where to **store** and **publish** digital information.
 - a. **Teams (including SharePoint)** – this is our main shared storage area for all business files. We have two instances – one for corporate IT users and one for schools, via Glow. See [Microsoft Teams and SharePoint](#) and [Sharing content in Glow](#) guidance.
 - b. **Shared network drive** – for databases we can't store on SharePoint. See [MS Access guidance](#).
 - c. **OneDrive for Business** – for storing small amounts of information that you can't keep in a shared storage area. See [OneDrive for Business User Guidance](#).
 - Only use your OneDrive to store the following.
 - Personal, work-related files. For example –
 - Work-related personal information such as Performance Review and Development (PRD) forms.
 - Personal employee documents relating to you or your team such as return to work paperwork.
 - Confidential information that you can't yet store in a secure shared area.

User responsibilities for managing digital information

- **Don't use your OneDrive to store any of the following.**
 - Your own personal files and media such as photos, music files and videos that aren't work-related.
 - Information you should store on Teams – someone may need it when you aren't available to share it with them.
 - Personal information on customers and service users.
- d. **Business function specific systems** – some services have dedicated systems that store and manage files relating to a particular function. For example
 - iTrent for employee files, and
 - Idox for planning and building standards files.
- e. **Other approved file sharing platforms** – to share files securely with other agencies. For example, Hyve for the Home Support service to share service user information with private service providers. Authorised signatories **must** request access for individuals through the [IT self-service portal](#).
- f. **InsideNL** – our corporate intranet, use this to publish files – generally control copies – in [document libraries](#) for all corporate IT users to access. Continue to store original working copies in Teams.
- g. **Websites** – to publish information publicly for wider audiences, mainly as web pages but also as downloadable files. Again, store original working copies of files in Teams.
 - For **all employees** including those who aren't corporate IT users.
 - [myNL](#) → [work well NL](#)
 - For the **general public** including our customers, service users and anyone else interested in the council.
 - [Council website](#) → [CultureNL](#) → [ActiveNL](#)
- h. **Viva Engage (also known as Yammer)** – our internal social networking platform. Ideally link to files on Inside NL or websites rather than store extra copies on here. This reduces the number of document locations you need to manage and makes sure users are accessing current versions.

4.4 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 users access to the systems and services they manage – in line with the relevant [Access control](#) and [code of connection](#) procedures.
2. As an authorised user, you have access rights to the IT assets you need to do your job and carry out your roles and responsibilities. You **must** use these rights appropriately.
 - a. Only use devices, IT systems, functionality, storage areas, folders, and files you're authorised to access; and
 - b. Never use unauthorised assets, for example, devices and software.

User responsibilities for the appropriate use of IT assets

3. Stay safe online when using search engines, visiting websites and other internet-based services. [Get Safe Online](#) is a useful website that includes:
 - a. [safe internet use](#) guidance;
 - b. tips to protect [your digital footprint](#);
 - c. the [check a website](#) tool to help you decide if a website is safe to visit; and
 - d. [online safety and security](#) advice.
4. Never create, store, view, download, or share (links and attachments) inappropriate content – inside or outside the council. This includes using search engines and websites, email, collaboration platforms, social media, or any other digital messaging facility to create, send, post, publish, reply, forward, or share communications that do any of the following.
 - a. Use language that is unprofessional, rude, vulgar, or otherwise unacceptable.
 - b. Insult, target or [discriminate](#) against people with protected characteristics,
 - c. Could be interpreted as
 - politically motivated,
 - bullying, harassment, victimisation, or inciting violence,
 - derogatory, abusive, indecent, obscene, or offensive, or
 - supporting illegal activities or criminal conduct.
 - d. Contain images, videos or written materials that:
 - are sexually explicit or exploitative; or
 - depict or promote discrimination, hate, violence, extremism or terrorism.
 - e. Send or post unsolicited or fraudulent messages. This includes the following.
 - **Spam:** That is, sending unwanted junk mail – usually sent to a lot of email addresses or social media group members – to try to tempt people into buying fake or unregulated products.
 - **Phishing:** That is, trying to exploit people into giving sensitive information, sending money, or clicking on an attachment or link that then installs malicious code such as a virus, malware, or ransomware.
 - **Assumed identity:** That is, sending messages while pretending to be someone else or claiming to be acting on their behalf, without their knowledge. The intention being to deliberately mislead people about who sent or authorised the message or any attachments. For example, by misusing a scanned signature or logging in to someone else's account.
 - f. Infringe copyright, while acting on behalf of the council – see the UK Government's [copyright information](#).
 - g. Operate or promote any private businesses and commercial ventures – including any owned by you, your family or friends.
5. **If you accidentally break any of these rules, you MUST tell your manager straight away.** If necessary – log an incident on the [IT self-service portal](#).
6. You must understand that we [investigate](#) all suspected inappropriate activity. For example –

User responsibilities for the appropriate use of IT assets

- a. [Inappropriate content and communications](#), as described in point 3 above.
- b. [Unauthorised personal use of IT assets](#) outwith the rules in section 4.8 below.
- c. Intentionally putting the council, our customers and service users at risk by:
 - disrupting or disabling network infrastructure, devices, IT systems or services;
 - installing or distributing viruses, malware, ransomware or malicious code;
 - accessing or distributing sensitive information without proper authority; and
 - downloading or distributing pirated software or stolen data.

4.5 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 4.4 above.
2. You **must** use the council email system for work-related activities.
 - a. Use your **individual council email account** for work and other approved organisational activities. For example, accessing employee benefits, applying for jobs through myJobScotland, and trade union activity.
 - b. Use a **shared email account** – where appropriate – to collectively manage team-level communications.
3. **Don't** do any of the following.
 - a. Send work related email or information to your own personal email address.
 - b. Send work related email or information to any other personal or external email address – except when corresponding with a member of the public or other third party, in line with points 2f and 2g of the [protecting information](#) guidance in section 4.2 above.
 - c. Use your council email address to send or receive personal messages – [except in emergencies](#) as detailed in section 4.8 below. You **must not** use it to do any of the following if they **don't** relate your job.
 - Sign up to email subscription and marketing services.
 - Use it as a contact address for any non-work-related online services and transactions. For example, personal shopping purchases and notifications, health and medical services, holiday, travel and event bookings.

Note: Our email filtering software may quarantine personal email messages like these as potential phishing. We will not release them to you. Read the [Email Security Guidance](#) for more information.
 - d. Use a non-council email address to send or receive work related messages. Exceptions to this are as follows:
 - Third parties operating on our behalf that **don't** have council email accounts.
 - IT systems that use independent messaging platforms for notification emails.
 - e. Edit the content of a third party's message, unless authorised to do so.

User responsibilities for using email

4. Be vigilant! Malicious email – including scam and phishing attempts – is our biggest IT security threat. Read the [Email Security Guidance](#) to find out how to spot and report suspicious email. In particular –
 - a. **If you have opened an attachment or clicked on a link in a suspicious email, don't panic!**
Report it to the IT Service Desk immediately on 0300 555 0406.
See the [Information Security Incident Management Procedure](#) for more details.
 - b. If an email seems suspicious, but you haven't clicked or opened anything.
 - Use the SCAM checklist to help you decide if it's malicious.
 - Click on the Phish Alert Report button in Outlook if you think it's a phishing email.
5. Read the following.
 - a. [Records Retention Schedule](#) for guidance on retaining and disposing of email messages and attachments.
 - b. [Information Classification and Handling Guidance](#) for rules on using email to share and send information to anyone:
 - inside the council or working on our behalf; and
 - outside the council, including partners and members of the public.

4.6 Using collaboration platforms

User responsibilities for using collaboration platforms

1. We use the following platforms to communicate, collaborate, chat, meet, share and store files, and access other IT products.
 - a. Corporate users – Microsoft Teams and SharePoint – see [user guidance](#).
 - This includes Viva Engage (also known as Yammer) and M365.
 - We also have a network share for files that aren't suitable for storage on MS Teams or SharePoint – mainly databases.
 - b. Teaching and schools staff – Glow (including Teams and M365).
See Glow [safety and security](#) and [Digital Learning and Teaching](#) guidance.
2. You **must** only access our collaboration platforms from council devices. **Don't** use [personal devices](#).
3. **Don't** store any of the following on [our storage facilities](#).
 - a. Personal files and media such as photos, videos and music.
 - b. [Copyrighted](#) materials and media.
4. You can join collaborative sessions hosted by other organisations via your browser using products such as Near Me, Webex and Zoom.

For any other products, you **must** request access through the [IT self-service portal](#). Give sufficient time for our technical staff to assess and fulfil your request.

User responsibilities for using collaboration platforms

5. Read the following.
 - [Information Classification and Handling Guidance](#) for information on storing and posting content on collaboration platforms, and
 - [Records Retention Schedule](#) for guidance on retaining and disposing of it.

4.7 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 – subject to the exceptions detailed in the [social media guidance note](#). This includes the following responsibilities.
 - a. Authorise every social media account and have administrative access to it.
 - b. Maintain a [directory of approved social media platforms and accounts](#).
 - c. Keep registers of owners and publishers – although services themselves are responsible for allocating owners and publishers.
 - d. Produce guidelines on the use of brand identity.
 - e. Deletes posts, comments or accounts that contain [inappropriate content or communications](#), as described in section 4.4 above.
4. Owners and publishers of council social media accounts **must**:
 - a. only use council devices;
 - b. follow the [Guidance on the use of social media for work purposes](#); and
 - c. never publish or share [inappropriate content or communications](#), as described in section 4.4 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 [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.

4.8 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 in the spirit of openness, trust and pragmatism. For example:
 - a. In urgent or emergency circumstances you may have to use council devices and systems to send or receive personal phone calls or email messages. See section 4.5 above for more guidance on [your responsibilities for using email](#).
 - b. General web browsing during breaks and lunch.
2. If you choose to make use of this privilege, you **must** follow these rules.
 - a. [Comply with all relevant council policies](#), including this one.
 - b. Personal use means just that. You **must not** use council IT assets for your or someone else's private business or commercial ventures.
 - c. Do it in your own time, not during work time. This limits you to before and after work, and breaks, including lunch.
 - d. It **must not** interfere with normal business or negatively impact your productivity.
 - e. You **must not** store personal files on any of [our storage facilities](#).
 - f. You **must** 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;
 - you are personally accountable for what you do with council IT assets, including online activity; and
 - if you abuse this privilege, we
 - reserve the right to withdraw it, and
 - will investigate your activity, where we suspect [potential misuse](#).

4.9 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 you **must not** attempt it.
2. We **don't** allow personal devices access to our cloud hosted systems and services – including [collaboration platforms](#), as detailed in section 4.6 above. However, there are exceptions to this, as listed below. Note: These are the only exceptions. You **must not** attempt to access any of our other cloud hosted systems and services using personal devices.
 - a. iTrent – to manage your own mySelf personal records only. Anyone with access to other people's records **MUST NOT** use their personal devices to view this information or process any employee management related workflows.

User responsibilities for using personal devices, software and cloud accounts

- b. **Viva Engage** (also known as Yammer) – to allow staff to read and contribute to conversations.
 - c. **Public facing websites** – viewing content on the [council website](#), [CultureNL](#), [ActiveNL](#), and the [myNL staff portal](#) and any other council owned sites. This does not include publishing functionality.
 - d. **Social media platforms** where we have a presence. As with publicly facing websites, anyone can view content we post on social media platforms but **you must not use a personal device when using social media for work purposes**, as detailed above.
 - e. **Microsoft Authenticator** – This is a free app you install on your personal device to authenticate onto the council network and M365 when working remotely.
3. You **must not** use software, systems or services that you have personally licensed, purchased, registered an account with, or subscribed to, for work purposes. This includes the following.
- a. Software installed on a personal device.
 - b. Cloud hosted systems and services such as M365, Adobe, [email](#), that you access from any device – personal, public use, or council managed.
4. We generally allow personal mobile devices in shared workplaces.
- a. In consideration of those around you and for your own privacy, set sound mode to low volume and or vibrate, and if possible, take calls where you won't be overheard.
 - b. Some specific work settings may have alternative standards of use for privacy or health and safety reasons.
This may mean you're not allowed to use your mobile device, have it visible or even on your person. For example: in customer facing roles such as teaching, in public facing roles, and social health and care settings.
Make sure you know the rules. Ask your line manager if you're not sure.

4.10 Reporting information security incidents

User responsibilities for reporting information security incidents

1. **Report it straight away to the IT Service Desk on 0300 555 0406 and or the Data Protection Team, and to your line manager if:**
 - someone has logged on to a device or system using another person's details;
 - a device is lost or stolen; and or
 - there may be a system or data breach.
2. Depending on the type of incident, you may also have to report it to one or more of the following.
 - your chief officer
 - your service's data protection officer

User responsibilities for reporting information security incidents

- the Information Security and Risk team
 - the Data Protection team and or the Corporate Data Protection Officer
 - the Information asset owner and or administrator
3. For full details see the following.
- [Information Security Incident Management Procedure](#)
 - [Data Protection Breach and Incident Management Protocol](#)

5 Monitoring

5.1 Monitoring activities and privacy

We carry out a range of monitoring activities on our IT assets to do the following.

- Comply with our regulatory and statutory obligations.
- Maintain the effectiveness of our IT assets.
- Prevent and or detect unauthorised use, criminal activity, and any other threats.
- Assure compliance with our policies, standards and procedures.
- Review and understand usage for operational, performance and maintenance reasons.

A note on respecting individual privacy.

The Acceptable Use of IT 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](#)

Council IT assets are primarily for business use, but we do allow some [personal use](#) as defined in section 4.8 above. In using our IT assets for both business and personal purposes, you **must** understand that 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 – including email and internet activity. and
- don't routinely monitor individuals but may access personal information as part of our monitoring activities.

As such, when using our IT assets, you:

1. can't presume privacy whether using them for business or personal reasons; and
2. agree to [comply with the Acceptable Use of IT Policy](#), including consenting to our monitoring procedures.

5.2 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 includes user activity such as where and when they access and use our IT assets. It does not log content, only information about the activity itself. 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 you create, modify, access, view, and receive. Examples include the following.
 - Files such as documents and spreadsheets.
 - Email messages and attachments, even if they've not yet been opened or received by the intended recipient.
 - Records and attachments in IT systems.
 - Websites including individual webpages and digital media.
 - Digital communication systems and services, including social media posts, comments and chats.
 - Anything displayed on a screen.

5.3 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 the

- [Acceptable Use of IT Policy](#), and or
- codes of conduct for [Councillors](#) and [Employees](#).

Managers MUST have formal approval before they can request access to individual user monitoring information, as listed in the table below.

Formal approval authority

- A Chief Officer **must** approve requests for employees within their service.
- The Deputy 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, Deputy Chief Executive or Councillors.
- The Leader of the Council **must** approve request for the Chief Executive.

Once approved, managers **must** use the [IT self-service portal](#) to make their request.

- **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. Reasons include the following.
 - Where we believe there is or has been a breach of this policy.
 - To comply with the request of law enforcement officers.
 - To comply with legal obligations.
 - To prevent or detect breaches of criminal or civil law.
 - 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 finishes.

1. The Chief Executive or the Leader of the Council, as per the formal approval authority above.
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.

6 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 location key

I = InsideNL intranet C = Council website or IT system we use E = External website

Product type	Product
Policies	<ul style="list-style-type: none"> ▪ Acceptable Use of IT Policy I ▪ Information Security Policy I ▪ Payment Card Data Security Policy I

Product type	Product	
Standards	<ul style="list-style-type: none"> ▪ Information Classification and Handling Standard 	I
Procedures	<ul style="list-style-type: none"> ▪ Information Security Incident Management Procedure ▪ Access control procedures ▪ Code of connection procedures 	I I I
Guidance	<ul style="list-style-type: none"> ▪ Email Security Guidance ▪ Home Working and Information 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) 	I I I I I
Related products	<ul style="list-style-type: none"> ▪ ActiveNL ▪ Corporate Communications Strategy ▪ Council website ▪ CultureNL ▪ Data Protection Breach and Incident Management Protocol ▪ Data Protection Policy ▪ Data protection subject access requests ▪ Digital and IT Strategy ▪ Discipline Policy and Discipline Guidance Note ▪ Employee Code of Conduct ▪ Freedom of information requests ▪ Full directory of social media networks ▪ Get Safe Online ▪ Get Safe Online: Check a website ▪ Get Safe Online: Online safety and security ▪ Get Safe Online: Safe internet use ▪ Get Safe Online: Your digital footprint ▪ Glow Digital Learning and Teaching Guidance ▪ Glow policy documents ▪ Glow safety and security ▪ Guidance on the use of social media for work purposes ▪ InsideNL document libraries ▪ IT self-service portal ▪ MS Access guidance ▪ Microsoft Teams and SharePoint User Guidance ▪ myNL ▪ OneDrive for Business User Guidance 	C C C C I I I C C C C C C E E E E E C C C C I C I I C I

Product type	Product
Related products (continued)	<ul style="list-style-type: none"> <li data-bbox="448 327 1426 360">▪ Public use of IT resources and the internet in libraries C <li data-bbox="448 371 1426 405">▪ Records and Information Management Policy I <li data-bbox="448 416 1426 450">▪ Records Retention Schedule C <li data-bbox="448 461 1426 495">▪ Sharing content in Glow C <li data-bbox="448 506 1426 539">▪ Viva Engage (also known as Yammer) User Guidance I <li data-bbox="448 551 1426 584">▪ work well NL C
Legislation, regulations, and government guidance	<ul style="list-style-type: none"> <li data-bbox="448 618 1426 651">▪ Copyright information: GOV.UK E <li data-bbox="448 663 1426 696">▪ Councillors' Code of Conduct E <li data-bbox="448 707 1426 741">▪ Discrimination: your rights: GOV.UK E <li data-bbox="448 752 1426 786">▪ Data Protection Act 2018 E <li data-bbox="448 797 1426 831">▪ Human Rights Act 1998 E <li data-bbox="448 842 1426 875">▪ Regulation of Investigatory Powers Act 2000 E <li data-bbox="448 887 1426 954">▪ Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 E