NORTH LANARKSHIRE COUNCIL
COMHAIRLE SIORRACHD LANNRAIG A TUATH

ACCEPTABLE USE OF IT POLICY

VERSION 5.11, JULY 2026

LIVE
LEARN
WORK
INVEST
VISIT

Document control			
Title	**Acceptable Use of IT Policy**		
Owner	Chief Officer (Legal, Democratic and Strategy)	**Contact**	InformationRiskAndAssuranceTeam@northlan.gov.uk
Governance group	Data Governance Board		
Author	Information Compliance Officer	**Contact**	InformationRiskAndAssuranceTeam@northlan.gov.uk

Revision history

Number	Originator	Date review commenced	Revision description/record of change
5.1	Information Risk Manager	10 June 2026	Changed Chief Officer title due to organisational restructure, provided additional clarification to section 6.8 – Using artificial intelligence, added links to six new quick guides, and made minor formatting changes.
5.0	Information Risk Manager	21 October 2025	Two-yearly review and change of writing style from second to third person.
4.0	Information Risk Manager	16 February 2023	Two-yearly review and plain English changes.
3.0	Information Risk Manager	June 2021	Updated link to home working guidance on MyNL.

Document approvals

Number	Governance group	Date approval granted	Date approval to be requested (if document still draft)
5.0	Finance and Resources Committee	27 May 2026	
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)

Status of document consulted upon	Stakeholders consulted between 24 October 2025 and 07 January 2026	
Stakeholders consulted and dates	Data Management and Compliance Group Technical Design Authority People Resources JNC for Teaching Staff Joint Trade Unions Data Governance Board	24 October 2025 24 October 2025 29 October 2025 26 November 2025 26 November 2025 07 January 2026

Strategic alignment

Plan for North Lanarkshire

Improving North Lanarkshire's resource base – Build a workforce for the future capable of delivering on our priorities and shared ambition.

Strategic alignment

Digital and IT Strategy

The Digital and IT Strategy is critical to enabling the Council to deliver on its vision. It sets the standards and provides the direction for the strategies, policies, and plans which enable the delivery of critical public services, business as usual activities and the investment programmes of work. 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 its IT users to risks.

Next review date

Review date	June 2028

Contents

1 Introduction

North Lanarkshire Council (the Council) uses information technology (IT) to work flexibly and efficiently to deliver services, carry out statutory duties, and support internal business functions. This policy informs its users on how to use IT assets appropriately.

The Council uses the following three types of IT assets – see the Acceptable Use of IT Guidance for examples of each.

1. **Computing devices** to access digital information and IT systems – in council offices and facilities, and other remote locations.
2. **IT systems and services** to process and store digital information and deliver services – hosted within its IT network and cloud-based.
3. **Network infrastructure and services** to access, store, manage and protect its digital information and IT systems.

The Council owns all information stored on its IT assets and on third party solutions managed on its behalf.

---

2 Purpose

This Acceptable Use of IT Policy provides a safe framework for using IT assets without exposing the Council or its IT users to unwanted risks. It is a corporate risk control factor and aligns with the following.

- Digital and IT Strategy – this brings together separate but related plans and policies – including this one – that contribute to the Council's digital vision.
- **Information governance policies** – Data Protection, Information and Cyber Security, Payment Card Data Security, and Records and Information Management – that keep Council IT assets safe and operational, and maintain information confidentiality, integrity and availability .
- **Codes of conduct** that set out mandatory standards for Councillors, Chief Officers, and Employees.
- **Legislative and regulatory compliance obligations and guidance.** This includes:
  - Computer Misuse Act 1990
  - Copyright, Designs and Patents Act 1988
  - Data Protection Act 2018
  - Ethical Standards in Public Life etc. (Scotland) Act 2000
  - Freedom of Information (Scotland) Act 2002
  - General Data Protection Regulations

- Human Rights Act 1998
- Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping purposes) Regulations 2018
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

3 Scope and exclusions

3.1 In scope

This policy applies to the following.

1. **All IT assets** – systems, services, and devices – that the Council uses to store, process, transmit or receive information.
2. **All digital information assets** – data, records, and files such as documents, audio, video, images – that IT users create or receive from third parties, process and store – within the Council IT network, on cloud-based services; or on removable media.
3. **Every person who creates, accesses, processes, and otherwise uses IT and digital information assets on the Council's behalf or in an official capacity.** This includes all employees, elected members, contractors, consultants, third-party suppliers and service providers, temporary agency staff, modern apprentices, students, volunteers, and anyone else with authorised access.

3.2 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 and Compliance Group** 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 Legal, Democratic and Strategy** – as the Council's Senior Information Risk Owner – is **accountable** for its governance.

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

1. Produce, publish and promote this policy.
2. Give guidance on how to apply and comply with this policy through standards, procedures and guidance – see product set for list and links.

3. Review every two years, with other reviews when needed. For example, following a critical security incident, new legislation, a significant threat, or an audit action.
4. Report to management teams, governance and working groups, committees and scrutiny panels.

5 Policy compliance

By using Council 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 the Council monitors usage of all its IT assets, and consenting to this monitoring.

Only use Council managed or approved devices to access IT systems and digital data, deliver services and conduct Council business – subject to limited exceptions.

The Council investigates any suspected breach of this policy, under the Discipline Policy and any other relevant policies. It refers any suspected unlawful acts to the appropriate authorities. This includes Police Scotland, and professional and regulatory bodies.

6 Acceptable use of IT assets

All users of the Council's 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 and secure access
2. Protecting digital information
3. Managing digital information
4. Appropriate use of IT assets
5. Using email and other digital messaging services
6. Using collaboration platforms
7. Using social media
8. Using artificial intelligence
9. Personal use of IT assets
10. Managing third party access
11. Using personal devices, software and cloud accounts
12. Remote access
13. 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 IT and information assets. The following quick guides are also available.

→ Quick guide to appropriate digital communications
→ Quick guide to appropriate use of IT assets
→ Quick guide to investigating potential misuse of IT
→ Quick guide to personal use of council IT assets
→ Quick guide to using artificial intelligence
→ Quick guide to using council and personal devices, software and cloud accounts

The Information Risk and Assurance team can help with questions about this policy and associated guidance:

✉ anyone can send an email enquiry; and
? employees with access to Viva Engage can post a question on the Information and Cyber Security community page.

6.1 IT authentication and secure access

User responsibilities for IT authentication and secure access
1. Use the most secure authentication method available for each system. This includes biometrics, multi-factor authentication, PINs and passwords. 2. When using passwords, use the three random words approach to make sure it's strong and unique. 3. Secure passwords and other secret information. Don't write them down and make sure no one can see when typing them in. 4. Never share credentials with anyone – protect usernames, passwords and other secret information. 5. Pick memorable information and security question answers that aren't easily guessable, if a system uses these as a secondary authenticator. 6. 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 – when working in Council offices and facilities, at home or another remote location, and in public spaces. 2. Keep information safe. a. Use a headset wherever possible to limit what others can hear. 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 technology in a secure location.

User responsibilities for protecting digital information

e. Don't access information without 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 devices when leaving them for a short while but still using them:

Windows logo key + **L**.

i. Log out of devices and close them down when no longer using them.

3. Never upload or transfer information to unauthorised third party systems, services, products or web resources. This may breach the following.
   a. Security controls as outlined in the following sections of the Information and Cyber Security Policy.
      → 7.3. Operational security
      → 7.5. Third-party supplier and service provider security
   b. Data protection rules relating to sensitive information, as defined in the following sections of the Data Protection Policy.
      → 10. Privacy by design and Data Privacy Impact Assessments (DPIAs)
      → 11. Data protection incidents and breaches
      → 13. Documenting data processing activities
      → 14. Sharing information with other Council services and third parties
      → 15. Data sharing
      → 16. Transferring personal information outwith the UK or EEA

6.3 Managing digital information

User responsibilities for managing digital information

1. When creating, using, processing, storing, sharing and disposing of information, make sure it's in line with business need and complies with information governance policies.
2. Follow the rules set out in the Information Classification and Handling Security Standard and Information Classification and Handling Security Procedures. See the following quick guides for more information.

   Quick guide to classifying information
   Quick guide to information handling rules
   Quick guide to information handling actions
   Quick guide to remote working security

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 Council websites. The Information Asset Register details physical and electronic locations for the various types of information.
5. Avoid using USB storage devices. If there's an approved business need, only use authorised hardware encrypted devices.

6.4 Appropriate use of IT assets

User responsibilities for the appropriate use of IT assets

1. Devices must use the most up-to-date managed operating system. Install or schedule device and software updates as soon as possible, especially critical security updates. Follow the on-screen prompts.
2. When working in Council offices and facilities, use wired network connections for devices where possible.
3. 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.
4. Use access rights appropriately – in line with job roles and responsibilities.
5. Stay safe online when using search engines, visiting websites and other internet-based services. The Get Safe Online website provides advice.
6. Don't breach copyright. This relates to any online source – websites and downloadable files – including newspapers, periodicals, journals, magazines, government and industry publications, and ebooks.
    a. It is acceptable to share, access and bookmark **links** to online content, including through email and other digital messaging services, social media, collaboration platforms, InsideNL, Viva Engage, websites and browsers.
    b. It is **not** acceptable to copy, share, store, republish or print any of the **source content** itself or a photo or screenshot of it.
    c. Take particular care with news and media articles - **never** reproduce, save or print articles, including headlines and excerpts.
    d. Note that there are exceptions, including the following.
        - Public sector information licensed under the Open Government Licence.
        - Educational use of digital publications under the Copyright Licensing Agency schools licence.
7. Never create, store, view, download, or share (links and attachments) inappropriate content that does any of the following.
    a. Uses unacceptable language.
    b. Treats people in a way that breaches codes of conduct or the Dignity at Work Policy.
    c. Insults, targets or discriminates against people with protected characteristics.
    d. Could be interpreted as politically motivated, bullying, abusive, offensive, or illegal.
    e. Contains images, videos or written materials that are sexually explicit or exploitative, or promote discrimination, hate, violence, extremism or terrorism.
    f. Distributes unsolicited or fraudulent messages. This includes spam, phishing and assumed identity.
    g. Infringes copyright.
    h. Operates or promotes any private businesses or commercial ventures.
8. **If a user accidently breaks any of these rules, they must:**
    a. tell their manager straight away, in line with the Discipline Policy; and

User responsibilities for the appropriate use of IT assets

   b. **if necessary, log an incident on the** IT service portal.
9. Understand that the Council investigates all suspected inappropriate activity.

6.5 Using email and other digital messaging services

User responsibilities for using email and other digital messaging services

1. Never use email or any other digital messaging services – such as Short Messaging Service (SMS), Multi-Media Messaging Service (MMS), Direct Messaging (DM), Instant Messaging (IM), and business system chat facilities – to send or share inappropriate content or communications, as described in section 6.4 above.
2. Only use approved messaging systems for work-related digital communications.
3. If using both individual user and shared team mailboxes, send email messages from the most appropriate account.
   a. **Individual user** – for work and organisational activities.
   b. **Shared** – to collectively manage team-level communications.
4. Users must never do any of the following.
   a. Send work related information to their own personal email or messaging accounts.
   b. Send work related information to any other personal or external email or messaging accounts – 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 6.9 below.
      Note: Email filtering software may quarantine personal email messages as potential phishing. Technical administrators will not release them.
   d. Use a non-Council email account or messaging service 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.
5. Be vigilant! Malicious email – including scam and phishing attempts – is the biggest IT security threat. Follow the SCAM checklist and Email security guidance for help on spotting and reporting suspicious email. This also applies to all other digital messaging services.
6. **Users must phone the IT Service Desk straight away if they have opened an attachment or clicked on a link in a suspicious message.**
   See reporting information security incidents in section 6.13 below for more details.
7. Read the Records Retention Schedule for information on retaining and disposing of email and Information Classification and Handling Security Procedures for rules on sharing messages.

6.6 Using collaboration platforms

User responsibilities for using collaboration platforms

1. The Council uses Microsoft Teams and SharePoint to communicate, collaborate, chat, meet, share and store files, and access other IT products.
2. It also uses a dedicated committee meetings webcast portal. This has two functions.
   a. Remote attendance: Elected members, officers and other participants can attend meetings online if they are unable to attend in person. They must only use Council devices to do this, as per point 3 below.
   b. Improved access to the local democratic process: Interested parties, including members of the public, can view meetings in real time or watch later, at a time that suits them.
3. Users must only access collaboration platforms from Council managed or approved devices. Don't use personal devices as detailed in section 6.11 below..
4. Don't store personal files and media or copyrighted materials on Council storage facilities.
5. Users can join collaborative sessions hosted by other organisations on other approved browser-based platforms.
6. Read the Information Classification and Handling Security Procedures 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. Strategic Communications is responsible for the Communications and Engagement Strategy and 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 Strategic Communications team has authority over all Council social media accounts – 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 to manage and post content, 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 – the Council's private, internal social network – can post informal communications and comments. See user guidance.
6. See the Information Classification and Handling Security Procedures for rules on posting information on Council social networking sites.
7. For guidance on **personal use of social media** and individual rights and responsibilities relating to expressing personal views about North Lanarkshire Council, maintaining confidentiality, and professional and ethical conduct, read the following.
   a. #FollowMe2: A social media guide for elected members

User responsibilities for using social media

b. Councillors: Advice Note on Social Media
c. Councillors: Social Media Card
d. Employee Code of Conduct

6.8 Using artificial intelligence

User responsibilities for using artificial intelligence (AI)

1. AI is a support tool that can help enhance productivity and improve communications.
2. Be mindful when considering uploading or sharing sensitive information to AI systems.
   a. Seek advice from information asset owners before proceeding.
   b. Never upload, copy or type in sensitive information.
3. Only use approved AI systems and services. This includes Copilot through the Council's M365 tenancies.
4. Never upload or copy any Council data to unauthorised AI systems and services. Or otherwise use unauthorised AI services as per:
   a. Section 6.2.3 – Managing digital information; or
   b. Section 6.11.4 – Using personal devices, software and cloud accounts.

6.9 Personal use of IT assets

User responsibilities for personal use of IT assets

1. Council IT assets are primarily for business use, but it does allow appropriate personal use. For example:
   a. using 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.
2. Users who choose to make use of this privilege, must follow these rules.
   a. Comply with all relevant policies, including this one.
   b. Don't do it during work time. It must not interfere with normal business or negatively impact productivity.
   c. Don't store personal files on any of the Council's storage facilities.
   d. Don't use Council IT assets for private business or commercial ventures.
   e. Understand that:
      - the Council owns all information stored on its IT assets – both business and personal – and as such it may be in scope for disclosure in response to data protection subject access and freedom of information requests;
      - 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

User responsibilities for personal use of IT assets
▪ if a user abuses this privilege, the Council reserves the right to withdraw it and will investigate their activity if it suspects potential misuse.

6.10 Managing third party access

User responsibilities for managing third party access
1. There are legitimate business reasons for allowing third parties access to Council systems. For example – a. Partner agencies who deliver services on the Council's behalf. b. Third parties who temporarily need access including contractors, consultants, work placement students, volunteers. c. Third party service providers performing systems administration tasks. 2. This may include authorising access through devices managed by some third parties. For example, third party service providers performing remote troubleshooting tasks. 3. The Council manages third party access through Code of Connection procedures. 4. Authorised signatories **must** log requests for third party access through the IT service portal.

6.11 Using personal devices, software and cloud accounts

User responsibilities for using personal devices, software and cloud accounts
1. The Council doesn't allow personal devices access to its IT network, or any systems or services hosted there. There are no exceptions to this, and users must not attempt it. 2. The Council doesn't allow personal devices access to its 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 use personal devices to access any other Council systems and services hosted on the cloud. a. **iTrent** – staff can only manage their own mySelf personal records. b. **Public facing websites** – users can view content on Council websites. c. **Social media platforms** – viewing content on platforms where the Council has a presence. Users must not use a personal device when using social media for work purposes. d. **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.

User responsibilities for using personal devices, software and cloud accounts
4. For privacy and data protection purposes, the Council doesn't allow the use of personal devices to photograph or record (audio, video, typed, or digitally written) in the work environment. This includes laptops, tablets, mobile phones, digital notebooks, voice recorders and dictation devices, smart glasses or any other body worn devices with camera and recording capabilities. 5. The Council generally allows personal mobile phones 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. b. In some specific work settings, users may not be allowed to use personal mobile phones, have them visible or even on their person for privacy or health and safety reasons. Line managers can give more guidance on this.

6.12 Remote access

User responsibilities for remote access
1. The Council uses a Virtual Private Network (VPN) for remote access to its on-premises systems. This should auto-start on login and take users through VPN process. 2. Remote or permanent home workers may have to attend Council offices or facilities for critical or major updates that can only be applied when their device is connected to the wired network. The Council will communicate this in advance. 3. As stated in the Hybrid Working Scheme: a. Those participating in the hybrid working scheme are not permitted to work from abroad or from a holiday home or location. b. Permission to use laptops outwith the normal working environment must be sought from the line manager and should only be granted in exceptional circumstances. 4. Read the following for more information. a. Section 3.5 of the Information Classification and Handling Security Procedures b. Quick guide to remote working security.

6.13 Reporting information security incidents

User responsibilities for reporting information security incidents
1. 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 following. a. Information Security Incident Management Procedure

User responsibilities for reporting information security incidents
b. Data Protection Breach and Incident Management Protocol.

7 Monitoring

7.1 Monitoring activities and privacy

The Council routinely carries out a range of monitoring activities on its IT assets for compliance, security, operational, performance, and maintenance purposes.

Users can't presume privacy when using Council IT assets for business or personal reasons. They are consenting to Council monitoring procedures by using its IT assets and agreeing to comply with this policy. The Council:

- collects and records usage data to make sure its IT assets work correctly and securely;
- monitors information entering, leaving, or stored on its IT assets; and
- doesn't routinely monitor individuals but may access personal information as part of its monitoring activities.

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,
   - → General Data Protection Regulations, and
   - → Human Rights Act 1998.
2. Monitoring and scanning obligations under the
   - → Regulation of Investigatory Powers Act 2000, and
   - → Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

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. The Council restricts and controls 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

The Council reserves the right to formally investigate individual usage – by exception and under strict controls – to help identify prohibited use or misuse in breach of this policy and or codes of conduct.

For example –

- Use of unauthorised third party systems, services, products or web resources
- Inappropriate content or digital services.
- Suspicious access to its systems including successful log ins from unauthorised locations and countries.

Managers must have formal approval before they can request access to this information. Once approved, they must use the IT 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 elected members.

→ The Leader of the Council must approve requests for the Chief Executive.

- **Level 1 investigation: Inspecting user logs** – to determine if there has been a breach; and or there's 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, a confirmed or suspected breach of this policy, to comply with the request of law enforcement officers, or a confirmed or suspected employment contact breach by an employee.

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 they can't inform the individual. For example, where there is reason to believe that this would prejudice or compromise an investigation.

The Council will refer any suspected unlawful acts to the appropriate authorities. This includes the police, and professional and regulatory bodies. See the Discipline Policy for more information.

8 Product set

The table below lists products referenced throughout this document. This may include links to other file types, websites and IT systems.

- Those listed under strategies, policies, standards, procedures, guidance, and related products are Council products. As per the note at the start of this policy, there are no active hyperlinks to files and web services used exclusively by council staff and elected members.
- Those listed under other resources, and legislation, regulations, and government guidance are the responsibility of other agencies.

Product type	Product
Strategies	▪ Communications and Engagement Strategy ▪ Digital and IT Strategy
Policies	▪ Data Protection Policy ▪ Dignity at Work Policy ▪ Discipline Policy ▪ Information and Cyber Security Policy ▪ Payment Card Data Security Policy ▪ Records and Information Management Policy
Standards	▪ Code of Conduct for Chief Officers ▪ Employee Code of Conduct ▪ Information Classification and Handling Security Standard
Procedures	▪ Code of Connection procedures ▪ Data Protection Breach and Incident Management Protocol ▪ Information Classification and Handling Security Procedures ▪ Information Security Incident Management Procedure
Guidance	▪ Acceptable Use of IT Guidance ▪ Email security guidance ▪ Guidance on the use of social media for work purposes ▪ Hybrid Working Scheme ▪ IT Authentication (Password) and Secure Access User Guidance ▪ Quick guide to appropriate digital communications ▪ Quick guide to appropriate use of IT assets ▪ Quick guide to classifying information ▪ Quick guide to information handling actions ▪ Quick guide to information handling rules ▪ Quick guide to investigating potential misuse of IT ▪ Quick guide to personal use of council IT assets ▪ Quick guide to remote working security ▪ Quick guide to using artificial intelligence ▪ Quick guide to using council and personal devices, software and cloud accounts ▪ SCAM checklist ▪ Viva Engage user guidance ▪ Where to store your files

Product type	Product
Related products	▪ Authorised signatories ▪ Data protection subject access requests ▪ Freedom of information requests ▪ IT service portal ▪ Information and Cyber Security on Viva Engage ▪ Information Asset Register ▪ Public use of IT resources and the internet in libraries ▪ Records Retention Schedule
Useful resources from other agencies	▪ #FollowMe2: A social media guide for elected members: Improvement Service ▪ Get Safe Online ▪ Schools licence: Copyright Licensing Agency ▪ School policy documents: Glow
Legislation, regulations, and government guidance	▪ Computer Misuse Act 1990: GOV.UK ▪ Copyright, Designs and Patents Act 1988: GOV.UK ▪ Copyright information: GOV.UK ▪ Councillors Advice Note on Social Media: Standards Commission Scotland ▪ Councillors' Code of Conduct: Standards Commission Scotland ▪ Councillors Social Media Card: Standards Commission Scotland ▪ Data Protection Act 2018: GOV.UK ▪ Discrimination: your rights: GOV.UK ▪ Ethical Standards in Public Life etc. (Scotland) Act 2000: GOV.UK ▪ Exceptions to copyright: GOV.UK ▪ Freedom of Information (Scotland) Act 2002: GOV.UK ▪ General Data Protection Regulations: GOV.UK ▪ Human Rights Act 1998: GOV.UK ▪ Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping purposes) Regulations 2018: GOV.UK ▪ Open Government Licence: GOV.UK ▪ Public Records (Scotland) Act 2011: GOV.UK ▪ Regulation of Investigatory Powers Act 2000: GOV.UK ▪ Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000: GOV.UK ▪ Three random words: NCSC.GOV.UK