Acceptable Use of ICT (Information Communication Technology)

Version 2.1

ISO27001

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

North Lanarkshire Council	Version No 2.1	Oct 2015
Acceptable Use of ICT Policy	**ISO27001**	

Document Control

Organisation	*North Lanarkshire Council*
Title	*Acceptable Use of ICT (Information Communication Technology) Policy*
Creator	*ICT Security Manager*
Source	*Review of policies produced by other Local Authorities and Industry best practice.*
Owner	*ICT Security Manager*
Subject	*The Acceptable Use of ICT formalises uses of Information Communication Technology within North Lanarkshire Council.*
Protective Marking	*OFFICIAL*
Identifier	***20151020 Acceptable Use of ICT Policy***
Date Issued	*08/12/2015*

Document Amendment History

Revision No.	*Originator*	*Date of revision*	*Revision Description*
1.1	*Brian Teaz*	*14/05/2013*	*Regular Review*
2.0	*Linda Caldwell*	*01/09/2014*	*Review for social media, PSN and PCI compliance*
2.1	*Linda Caldwell*	*20/10/2015*	*Regular review*

Document Approvals

This document required the following approvals:

Sponsor Approval	*Revision No.*	*Date*
Information Governance Working Group	*2.1*	*26/11/2015*
Customer Services Development Working Group	*2.1*	*13/11/2015*
Human Resources/Trade Unions	*2.1*	*13/11/2015*
Information Security Forum	*2.1*	*17/11/2015*
Policy & Resources Committee	*2.1*	*03/12/2015*

Table of Contents

1 Introduction

1.1 Purpose

North Lanarkshire Council (the council) aims to help employees make the best use of the Information Communication Technology (ICT) systems and facilities. The use of ICT can bring significant benefits to council activities and delivery of services. However, it can also introduce significant types of risk to our operations. The aim of this policy is to provide a safe framework for using ICT without exposing the council or our employees to the risks which can come with its use.

This policy has been developed to:

- Ensure acceptable use of ICT by all users;
- Establish the parameters of appropriate use and best practice;
- Protect the council and users from potential legal liabilities;
- Explain the consequences of breaching acceptable use.

The Acceptable Use of ICT Policy is part of a group of policies and standards which complement the Information Security Policy.

1.2 Scope

This policy applies to all employees of North Lanarkshire Council, to third party organisations or contractors and to anyone else who is authorised to access and use council ICT facilities, systems and services. This includes councillors who have access to and use of such systems and facilities for the performance of their role as elected members. This policy does not apply to school pupils. For the purpose of this policy “employees” includes full-time, part-time, term-time and any temporary staff.

The policy relates to the use of:

- Council telephone systems, including fax machines and mobile phones;
- All computers including portable computers, all mobile communications devices such as tablets and all smartphones;
- All storage central and external;
- ICT systems such as business applications, e-mail and internet browsing.

1.3 Regulatory and Compliance Requirements

The council is required to comply with legislation, such as the Data Protection Act 1998 and many others. At all times users should act in such a manner as to protect the confidentiality of the information being processed in accordance with the Data Protection Act 1998. Further guidance on the requirements of data protection can be found in the following document: North Lanarkshire Council Data Protection Policy

The Acceptable Use of ICT Policy incorporates the main principles of relevant legislation, and this legislation is listed in Appendix C. There is also a requirement for compliance with a variety of Codes of Connection as a pre-condition for sharing information with government departments

or other public bodies notably the Public Service Network (PSN) code of connection. Similarly, the council's automated payments collections processes are governed by the Payments Card Industry Data Security Standard (PCI DSS). The onus is on North Lanarkshire Council to demonstrate and provide evidence of compliance for all of these regulations. The contents of this policy form part of the overall compliance requirements for the council.

1.4 Responsibilities

1.4.1 Executive Directors / Heads of Service

Executive Directors and Heads of Service have a specific responsibility for the implementation of the council's policies within their respective service.

1.4.2 Line Managers / Supervisors

Line managers and supervisors have a responsibility to ensure that:

- All employees within their teams are aware of and follow the terms of the policy and guidelines;
- Employees are made aware that e-mails, phone calls, internet usage and any electronic communication will be scanned (See section 1.***8***.1 Content Scanning);
- New employees are provided with the necessary information and training as part of the induction process;
- Appropriate training in the use of new ICT systems is provided to the council's employees;
- Consideration is given to training requests in relation to the use of the council's ICT systems;
- The leavers process is initiated when an employee leaves the council, or ICT are notified when an employee no longer requires access to a specific system.

1.4.3 Employees / users

Employees and users have a responsibility to:

- Familiarise themselves with the terms of the policy;
- Adhere to the terms of the policy and the supporting guidance material.

1.4.4 Third Parties

Council managers with responsibility for relationships with third parties who use council ICT systems must ensure that:

- Third parties are aware of the requirement to comply with this policy;
- Third parties are identified as such when requesting access to council systems;
- ICT are notified when a third party no longer requires access to a specific system;
- All third party contracts reflect the requirement to comply with council security policies.

1.5 Policy review and revision

This policy will be reviewed whenever guidance or the law is changed but at a minimum every 24 months. Policy review will be undertaken by the ICT Security Manager in consultation with the Information Security Forum, the Customer Services Development Working Group, Information Governance Working Group, Human Resources and the Trade Unions.

1.6 Training and Awareness

It is essential that users are given sufficient information and training to assist with compliance of the terms of this policy.

- A copy of this policy is available to all users of ICT systems;

To further reinforce the key policy requirements, guidelines are available and are part of the information security awareness action plan.

1.7 Business use, personal use and misuse of ICT

1.7.1 Business Use

The council's ICT facilities are a business resource provided to employees for work-related purposes.

Employees with official union responsibilities, and with agreement of their manager, may use council ICT facilities to discharge their union duties (not trades union "activities"), as this will be regarded as business use. This will be in line with Time Off for Trade Union Duties and Activities Guidance, Section 2, paragraph 2.4. The use of ICT facilities for personal or private purposes during working hours is not permitted, other than in the limited circumstances detailed below.

1.7.2 Personal Use

The council recognises that employees, from time to time, may need to deal with private business or personal matters during the course of their working day. In the interests of good employer/employee relationships, limited personal use of the telephone systems, e-mail, Lync (Skype for Business) and the internet is therefore permitted, in employees' own time subject to the following rules :

- Personal use of telecommunication systems will be permitted for urgent or emergency purposes only, including those occasions when employees are on council business away from home overnight;
- The use of the telephone systems, Lync (Skype for Business) or e-mail system for personal matters at any other time will require specific authorisation from the line manager, with the exception of council mobiles, which may be used out of hours and at weekends for general personal use. This is subject to a charge being levied for all personal calls, messages etc. The mobile phone number belongs to the council and will not be transferred to an employee. The personal use of council mobile phones for urgent or emergency purposes as set out above, during the working day in employees own time, e.g. lunchtime, would not incur a charge;
- The use of personal mobile phones must not interrupt work other than for emergency purposes;
- The internet may be accessed for personal use during employees' own time only e.g. lunchtime. Similar access restrictions will apply to that authorised for business purposes i.e. requests for access to blocked sites will only be actioned where required for business;
- Social media sites may be accessed for personal use during employees' own time only e.g. lunchtime. See section 6.5.3 for further information;
- Other private, recreational or commercial use or the advertising of goods and services by e-mail or on the internet are strictly prohibited.

Examples of such purposes are detailed in the Acceptable Use of ICT Guidelines.

1.7.3 Misuse

Misuse of ICT can cover any activity carried out using council ICT resources, for example:

Do not:

- Use ICT systems for any purpose which would reflect negatively on the council or its employees;
- Carry out any activity which would cause damage or disruption to council operations, or which would constitute a criminal offence;
- Create, transmit or disseminate material that may bring the council's name or the name of any of its employees into disrepute, whether on the council's own web site or externally;
- Break or attempt to avoid or break through council security controls;
- Undertake any activities that violate laws or rights of third parties, e.g. installation or distribution of unlicensed software, unauthorised copying of copyrighted material, storage of such materials on any of the council's systems;
- Acquire or transmit information or lists concerning council employees and disclose them to parties outside of the council, unless authorised to do so;
- Use council internet IDs, e-mail addresses and web pages for anything other than authorised communications;
- Send or deliberately receive credit or debit card numbers. If you do receive an email containg a credit or debit card number you must delete it immediately;
- Intentionally access, view or download pornography, or any type of illegal material or material which contravenes council policies;
- Access, retrieve, or print text and graphical information which exceeds the bounds of generally accepted standards of good taste and ethics or which contradicts the council's organisational values and/or employment policies;
- Carry out any freelance work unrelated to the council's business, gamble, contribute to internet newsgroups, play games (unless in a context of school curriculum activities) or conduct political activities;
- Exceed your contractual authority under the Council's Standing Order Regulations covering procurement;
- Carry out any activities which would incur significant unauthorised costs;
- Participate in peer-to-peer file sharing, streaming audio/video, instant messaging, unless expressly authorised by the council and managed securely through council ICT network facilities with agreement from the council ICT service[1];
- Store council information in an unauthorised external location e.g. cloud storage, non-council managed computers, non-council email;
- Intentionally access, execute or transmit malicious software e.g. viruses, worms, trojans, etc.

This list is not exhaustive, and any misuse of ICT systems may lead to disciplinary action in accordance with the Council's discipline policies i.e. Discipline Policy or JNCT Disciplinary Framework for Teachers as appropriate.

---

[1] *Streaming audio/video …. Instant messaging This does not apply to these technologies if used in an Educational/Curriculum context.*

1.7.4 General Controls

The use of analysis tools on the council's ICT systems, and other actions which can influence or impair system stability and security, must only be performed under the direction of the council ICT service.

Council computers may not be connected to another organisation's network without permission both from the council ICT service and from the organisation concerned. No sensitive council information may be accessed by council mobile devices when connected to public networks.

Employees should notify their supervisor or manager of any abuse of software or accompanying documentation. This must also be reported to the council IT Service Desk.

There may be some circumstances where for valid operational reasons some of the practices listed above may be authorised by the council. In these cases the policy exception request process should be followed**.** In the first instance policy exception requests should be referred to the service Information Security Forum representative. Details of the Information Security Forum representatives are available in Appendix A of the Acceptable Use of ICT guidelines.

1.8 Scanning and Monitoring

1.8.1 Content Scanning

Automated filtering systems are used for scanning electronic communications as a means of protecting against viruses or other security threats, and of detecting inappropriate content.

The automated systems maintain logs of inappropriate activity. These are available to senior managers for review.

1.8.2 Monitoring

Communications systems and content are not routinely monitored but monitoring may be used to allow managers to evaluate use of electronic systems. The results of this monitoring may be used to inform the council's disciplinary procedures.

As an exception, some council communications systems are routinely monitored for operational reasons**,** particularly those involving customer interactions. Two primary examples are the Customer Contact Centre and Housing and Social Work emergency services where telephone calls are likely to be recorded.

1.9 Violations of the Policy

Where it is suspected or established that an employee is abusing or misusing ICT facilities, such abuse or misuse may lead to the restriction or the withdrawal of any or all of the facilities.

Abuse or misuse may also be a disciplinary offence and any violation of the policy may result in disciplinary action in terms of the council's disciplinary procedures. Users should be aware that a significant breach of the policy may represent gross misconduct under the council's disciplinary procedures and could lead to summary dismissal. Violations could also amount to criminal offences and lead to prosecution.

1.10 Further Information

For further information, contact the service Information Security Forum representative or the ICT Security Manager. Contact details are provided in Appendix A of the Acceptable Use of ICT guidelines.

Alternatively, send an e-mail to SecurityPolicy@northlan.gov.uk

2 Use of ICT Equipment

ICT equipment is provided by the council for business purposes. It is provided under the conditions outlined below. This policy applies to all council provided ICT equipment.

2.1 General Rules

Do:

- Make sure your mobile ICT equipment is stored safely when travelling to minimise the risk of losing data;
- Handle storage devices as if they are valuable items. Carry with care!
- Report the loss or theft of any ICT equipment, including mobile devices, to your line manager and to the IT Service Desk at the earliest opportunity. Any potential loss of data must be recorded and reported;
- Regularly check mobile storage devices for viruses;
- If you store council information on mobile devices with the agreement of management, you must ensure that the information is suitably protected. If you are in any doubt seek advice from your manager, supervisor or the IT Service Desk. All laptops and tablets must be encrypted;
- Take care when using a mobile phone to avoid being overheard when discussing sensitive information or council business;
- Take care when using the video facility in Lync (Skype for Business) that no sensitive information is visible in the background;
- Take reasonable measures in handling mobile ICT equipment to protect against loss or theft as it may hold valuable or sensitive information;
- Follow the policies, procedures or instructions issued by your service to ensure that mobile phone use complies with Health and Safety and legal regulations.

Do not:

- Use equipment for any purpose other than for what it has been authorised;
- Use non-council ICT equipment for council business or to store council information unless authorised to do so;
- Enter or save a credit or debit card number in a council application or service or enter or save a credit or debit card number in council data. The exception to this is when paying by debit or credit card using an authorised secure payment service.
- Attempt to alter the configuration or settings on your ICT equipment unless authorised to do so;
- Load any personal software onto a council computer unless authorised to do so;
- Allow anyone other than yourself or other individuals authorised by the council to use your ICT equipment;
- Remove information from council premises without prior authorisation from management;

- Store sensitive council information on a mobile storage device;
- Use mobile storage devices as a means of transferring council information to non-council third parties equipment without prior authorisation from management;
- Use a USB memory stick for backing up your computer unless there are no other means of carrying out backups;
- Store passwords or usernames or any other sensitive information on your work mobile phone. Information on passwords can be found in the Acceptable Use of ICT Guidelines;
- Interrupt your work to respond to or send personal text messages unless for emergency purposes.

2.2 Purchasing ICT Equipment and Software

All council ICT purchases must follow the council procurement procedures. No such equipment may be purchased for private use by individuals. The council expressly forbids the use of any software which has not been purchased, licensed or authorised for use on council equipment or on approved hosted websites. Where it is proposed to host new or upgraded software externally i.e.on the cloud, a security assessment will be required to confirm that the software and external site meet council security standards.

2.3 Using Software and Installation of Software

Council ICT software and its documentation must not be reproduced, unless explicitly agreed by the council ICT Service.

Workstations should be configured to prevent users from being able to load software. This will safeguard licensing agreements and protect against the inadvertent installation of malicious code. Only properly licensed and/or authorised software may be loaded onto any council computer. Software includes business applications, shareware, entertainment software, games, screensavers, and demonstration software. There may be valid instances where unlicensed software or shareware is legitimately available for use by the council. In these instances downloading, installation and use must be for authorised purposes only.

Only those authorised by the council should be allowed to install software.

2.4 Disposal of Old Equipment and Repairs

ICT equipment may store sensitive information. Information can be retrieved using simple tools, freely available on the internet. During repair or disposal, it is important that all equipment is handled and, if necessary, disposed of safely. The council has a specific process to dispose of media safely and securely. This process must be followed and can be initiated by contacting the IT service desk. If you require advice on this, contact the council IT Service Desk.

3 Access to Council ICT Systems

Access to council ICT systems and information is provided on the basis that users are given a level of access required to enable them to carry out the work they are authorised to do.

3.1 General

Access to council ICT systems and software applications is controlled through the use of user accounts and passwords.

Levels of access to ICT systems and information should be limited to the role and activities that the user has been authorised to do.

Guidance on remote or home-working should be sought from your line manager in the first instance**.** Remote access to council ICT systems on the corporate network is only permitted from council managed devices. On the schools network remote access is permitted from both council and non-council devices. Further information is available in the Acceptable Use of ICT Guidelines.

Staff must only enter (or direct others to enter) credit/debit card numbers and associated security codes into approved PCI DSS compliant payment devices e.g. approved tills and PDQ devices, or approved online payment applications and web interfaces using secure and approved computers. Credit/debit card numbers and associated security codes must never be written down on paper, typed into emails, stored in spreadsheets or other documents, or entered into unapproved ICT systems.

3.1.1 General Rules

- Access to each ICT system must be managed by User Identifiers (User IDs or User Names) and passwords;
- ICT systems must not pre-populate logon screens with user identifiers;
- Access to ICT systems and user access maintenance for ICT systems commonly available to all users are the responsibility of the council ICT Service. This will include network logon, e-mail, network printing facilities, centralised file storage areas, backup, etc;
- Access to council business software applications and user access maintenance are the responsibility of the services' ICT systems owners and nominated ICT systems administration teams;
- Systems owners must define which levels of access are authorised to which groups of users. These are known as "Access Control Policies";
- There must be procedures in place to regularly review user access, to ensure that users who no longer require access, are removed.

Do:

- Log-off / lock your screen when you are going to be away from your desk for a period of time;
- Keep your password confidential;
- Change your password regularly;
- Follow the password advice in the Acceptable Use of ICT Guidelines.

Do not:

- Disclose your password to anyone – not even to the council's ICT service, support team or IT Service Desk;
- Let anyone else log on to a computer or application using your user identifier (or user name). The user identifier is your identifier and you may be held responsible for all actions undertaken by that user identifier;

- Save credentials e.g.user identifiers, passwords, account details, etc in web browsers.

3.2 Virus Protection

The council has ensured that on all council ICT systems continuous protection is enabled by approved virus scanning software with a current virus database. This virus-software must not be de-activated.

In order to minimise the risk of viruses entering the council's ICT systems, employees must not load unauthorised software onto any council ICT system or download software from the internet. Further clarification in terms of such files may be obtained from the council IT Service Desk.

Generally, more damage to files can be caused by inappropriate corrective action than by viruses themselves. Any incidents must be reported immediately to the council IT Service Desk or the ICT Security Manager.

3.3 Backups

The central servers are backed up on a regular, scheduled basis, and the backup media are securely managed, even when off site. You should store data centrally on servers, not on a local personal computer. For corporate users a “home” directory on one of these servers is provided for that reason. Even if you make local copies for backup purposes, your management of them will fall outside of the standard, audited and managed, central processes.

If there are specific reasons why you must store data locally, advice on how to do this must be sought from the council IT Service Desk.

3.4 Printing and its Security Implications

When printing sensitive information you must make sure that you can pickup the printouts immediately. Great care must be taken if you print confidential information on printers located in areas accessible to many people. The same care should be taken with faxes received on council fax machines. Extra care must be taken if printing outwith council premises or at an unfamiliar council location.

4 Using Council Information

4.1 Intellectual Property and Copyright

- Each user of council ICT systems must surrender all council information on leaving employment. No copies may be retained for personal use;
- You are not allowed to use within the council any material that you either know, or suspect to be, in breach of copyright;
- You are not allowed to pass such material on to anyone else;
- You must appreciate that all information offered on the internet is protected by property rights. You must gain appropriate usage rights before using such material.

4.2 Non-Disclosure

Council information of a personal, confidential or commercially sensitive nature must not be disclosed to anyone unless authorised by an appropriate council officer. Information must be treated as a valuable asset and handled accordingly.

4.3 Use of Information Accessed

Employees that have access to sensitive or personal information from any source, must only use the information gained for its intended purpose. Violation of this principle may not only breach the terms of this policy but also Data Protection legislation which protects confidentiality. Violation of either or both could constitute gross misconduct.

4.4 Information Published on the Internet

Council-related information published on the internet, websites, blogs, social networking sites or on any other publicly-accessible media, must be authorised by Corporate Communications prior to publication.

4.5 Information Classification and Data Handling

North Lanarkshire Council will define how information should be classified and labelled in terms of the degrees of privacy and confidentiality to be applied.

These classifications will determine how each class of information should be stored, managed, handled and shared.

The information classifications are available in the Information Handling policy and align with the Government Security Classification policy.

4.6 Information Storage

Information should only be stored on encrypted portable computers as a temporary measure. Documents, folders, files and any other form of council or client-related information should not be permanently stored on portable computers or other mobile storage devices.

This type of information should be permanently stored within central storage facilities provided by the council within the boundaries of the council network e.g. on fileshares such as H:/ or I:/ drives, on Connect or in EDRMS. Information stored outwith this central storage requires additional resource when the council needs to respond to FOI or Subject Access Requests.

Any exceptions to this rule must be authorised and justified by the service on the basis of risk.

5 Using E-mail Facilities

5.1 Introduction

E-mail provides employees and the council with a speedy, convenient and efficient means to communicate information.

5.2 General Rules for e-mail

Do:

- Manage your e-mail to ensure you do not exceed the standard e-mail limits for capacity;
- Be aware that all e-mail correspondence is logged and stored and will be made available for investigation of inappropriate use or content which may result in disciplinary action;
- Report inappropriate use or content to your line manager;
- Delete any suspicious messages received from unknown sources.

Do not:

- Send messages using other user's accounts unless authorised to do so e.g. sent on behalf of… ;
- Forward an e-mail from an address or person you do not recognise;
- Automatically forward e-mail from a council mailbox to a private one. There is no guarantee that the e-mails forwarded do not contain sensitive or personal information and there is no protection for the content once e-mails leave the council network and go out over the internet;
- Use language which might cause offence or be seen as abusive, discriminatory, bullying in nature or harassment;
- Send or forward jokes, chain letters or other offensive or inappropriate content;
- Send files or documents from a computer that does not have up to date anti-virus and malware protection;
- Use a scanned version of a handwritten signature to sign an e-mail;
- Give out personal information or confidential information unless authorised to do so. Further guidance is available in North Lanarkshire Council Data Protection Policy;
- Conduct your own personal business activities.

This list is not exhaustive, and the council reserves the right to take action against an employee who, in the reasonable opinion of the Council, has abused the system.

5.3 Large Files and Attachments

Avoid attaching large or multiple files to an e-mail. Where possible use shared storage areas and send a link to the file(s).

The maximum message size varies according to the email system being used:-

GCSX	4 MB
Exchange	10 MB
FirstClass	20 MB

It should be noted that this maximum will include the message headers and could therefore be up to 1 MB lower.

If you have to send large files externally you should be aware that large files may be delayed for sending until after 6.00pm each evening.

5.4 Large Distribution Lists or Group Messages

Individual users must not send out messages to large groups of users without first seeking appropriate approval and then following the correct procedures for doing so.

Corporate Communications control council address groups whereas individual services control those lists specific to them.

5.5 Mailbox Access

Users should be aware that access will be provided to individual mailboxes in relation to business activities in their absence or as a result of their termination from the organisation.

Permission must be sought from an appropriate senior manager for such activities.

5.6 Sensitive Information

The privacy and confidentiality of messages sent via e-mail cannot be guaranteed.

Users are advised that all external e-mails have a disclaimer at the footer of the e-mail to protect North Lanarkshire Council from information being disclosed to unauthorised personnel.

However, there is no guarantee that this will protect individual personnel from potential legal action if e-mail sent includes unsupported allegations, sensitive or inappropriate information.

It is the responsibility of all users to exercise their judgement about the appropriateness of using e-mail when dealing with sensitive subjects.

When sending sensitive information by e-mail, an appropriate protection method must be employed to ensure the security of the information. Further information is available in the Information Handling policy.

5.7 GCSX e-mail

The GCSX e-mail system is a system hosted on behalf of the Government to provide secure e-mail transmission between subscribing public bodies only. It cannot be used to send secure email to any other organisation or individual. It operates alongside the council e-mail system. As it is a secure system its use is covered by additional regulation with which the council, as a subscriber, has agreed to comply. Rules covering use of GCSX can be found in Appendix B.

6 Using the Internet

6.1 Introduction

The internet provides a valuable source of information for the council and for employees. The

council recognises the value of the internet as a source for information and as an excellent means of communicating quickly to a wide audience.

At the same time the internet is largely unregulated and it must be used with caution. It can be a source of security threats, and information available from it may not be reliable, up-to-date or accurate.

It is to be used in a manner that is consistent with the council's values and standards of business conduct, and as part of the normal execution of job responsibilities.

6.2 Good Practice When Using the Internet

Whilst the council recognises the value of the internet as a resource for information, it is easy to spend large amounts of time searching for information, and very easy to become distracted in the activity.

For further advice on web browsing refer to the Acceptable Use of ICT Guidelines.

6.3 Use of Council Internet Facilities

Do:

- Exercise caution when surfing unfamiliar or untrusted websites;
- Be specific in your use of words when using search engines;
- If you accidentally discover a website which contains any material which could be judged to contain sexually explicit, racist, violent or any other potentially offensive material, disconnect from the site immediately. Report this to your manager or supervisor;
- Report anything suspicious to council IT Service Desk;
- Manage your time spent browsing.

6.4 Blocked Websites

Where websites have been blacklisted they will not be unblocked unless there is a valid business or educational requirement for this.

Requests for access to blocked websites require service authorisation.

6.5 Social Networking and Blogging

6.5.1 Overview

Social media is the use of web-based and mobile technologies where users can easily participate in discussion, and share and create content. It includes, but is not limited to, popular sites such as Facebook, Twitter, MySpace, YouTube, Flickr and blogs hosted on sites such as Blogger and WordPress.

6.5.2 Official council social media sites

Some employees are permitted to make use of social media facilities as part of their jobs, to inform service users about council services and to respond to requests for service. Any such employee must do so in a professional manner which is consistent with the Employee Code of Conduct and organisational values.

Employees permitted to make use of social media facilities as part of their employment should be aware that, as well as being personally liable for any content posted, the employer may also be liable for the actions of employees.

No employee should create a social media page/site purporting to be an official council page/site without permission from the Head of Corporate Communications or an officer nominated by them. The exception is Learning and Leisure Services staff in schools who are authorised to create a social media page or blog as part of a learning and teaching environment or as a communication tool, providing they notify Corporate Communications.

The Head of Corporate Communications may direct that any social media page/site purporting to be an official council page/site but which is unauthorised be deleted.

Where the use of such a page/site is approved, Corporate Communications staff will advise on look and tone of content and will have responsibility for ensuring look and tone of content complies with council standards.

The council uses third-party software to manage its social media presence. Any new official page/site will be required to be managed using this software. Corporate communications will provide suitable training to named officers within the commissioning service who will be responsible for updating the relevant page/site. Licence costs for new users will require to be met by the commissioning service.

There is an exception for Learning and Leisure Services staff in schools where social media is used as part of a teaching and learning environment or as a communication tool.

6.5.3 Employee use of social media

The council allows access to social networking sites for personal use from our computers in employees' own time, e.g. lunchtime.

Employees must at all times comply with the council's Employee Code of Conduct and demonstrate adherence to the council's organisational values. Any misuse of ICT systems may lead to disciplinary action in accordance with the Council's discipline policies.

Employees should familiarise themselves with the guidance on the use of social media, in the Acceptable Use of ICT Guidelines.

6.6 Information Reliability

All information on the internet should be considered suspect and valued accordingly when used in council's processes. Only use information provided by sites which you trust.

6.7 Copyright

Upload or download of materials must be within the confines of copyright law. You must not upload, download, or otherwise transmit commercial software or any copyrighted or suspected copyrighted materials belonging to parties outside of the council, or the council itself. Download of media files such as music and video (e.g. mp3, mpeg, avi, etc) files is prohibited unless within copyright law. The council may remove non business-related or unauthorised files periodically as

a matter of policy. If in doubt, advice should be sought from your line manager, supervisor, IT Service Desk or the ICT Security Manager.

6.8 Guest Access to the Internet

This section specifically refers only to non-council employees who require temporary access to the internet.

- The council provides guest access to the internet for visitors, partners, contractors, etc through the council's IT Service Desk. This should be requested in advance. This is via a controlled wireless service (WiFi). This is not a service provided on a standard council desktop PC.
- Council ICT systems may be used to provide guest access to the internet. However:
    - A level of service will not be guaranteed;
    - Satisfactory quality or performance cannot be guaranteed;
    - The risk of poor accuracy, and loss of user's data[2] is with the user.
- Guest users will only be provided guest access to the internet for purposes agreed by the council.

Access may be authorised for council staff in exceptional circumstances.

7 Security Incidents

Users must immediately report to their manager or supervisor when:

- Information in any form has, or is suspected to have been lost or disclosed to unauthorised parties;
- Unauthorised use of council's information systems has taken place, or is suspected of taking place;
- Passwords or other systems access control mechanisms are, or are suspected of having been lost, stolen, or disclosed.

The council IT Service Desk must be contacted immediately about unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages, etc.

Service managers or supervisors, on being notified of a potential security incident, must agree the appropriate course of action to be taken with the council ICT Security Manager.

Details of security incidents or suspected security incidents must be treated as "OFFICIAL–SENSITIVE:LOCSEN" and only discussed with those parties engaged in the council's investigation process (See Information Handling Policy for further information).

When a security incident is suspected it is very important to report it as quickly as possible. The

[2] *"Loss of user's data" in this context refers to data owned by the user and not Council data.*

earlier an incident can be identified and its impact assessed the greater the chance of dealing with it successfully.

Further information is available in the Information Security Incident Management procedure.

All breaches of the Acceptable Use of ICT Policy must be reported to your service management. If you suspect that a fellow employee is abusing or misusing council systems you should, in the first instance, contact your line manager or supervisor. If the misuse or abuse is being carried out by your supervisor or line manager you should report it to his/her manager. If you have serious concerns about illegal conduct or behaviour, you may refer to the council's Whistleblowing Procedure .

Appendix A: Glossary of Terms

Term	Description
Blogging	Writing a blog. A blog (short for weblog)is a personal online journal that is frequently updated and intended for general public consumption.
Central Storage	See Shared Area
Cloud Computing	Alternative model for providing ICT services via the Internet rather than locally. Although there are many advantages of cloud computing, care must be taken to ensure that security is not compromised
Communications Systems	In the context of content scanning communications systems refers exclusively to internet browsing and e-mail use.
Confidentiality	Information confidentiality is the need to restrict access to information, only to those who have authorisation or a right to access it.
Content Scanning	Content scanning is the use of automated software tools to detect viruses, dangerous software or inappropriate content within e-mail and internet communications systems
Council ICT service	The areas which provide, manage and support ICT facilities and resources for the council
Disciplinary Action	Any disciplinary action taken in relation to a breach of the Acceptable Use of ICT Policy will be in line with council Disciplinary Procedures.
External Storage	Storage that connects to individual computers e.g. DVDs, memory sticks, cameras and external hard drives.
ICT	Information Communications Technology
ICT Equipment	ICT Equipment includes all types of computers; telecommunications devices such as telephones, mobile phones, smartphones, faxes and storage devices such as CDs, DVDs, USB memory sticks and all manner of mass-storage devices and portable disk drives.
ICT Systems	**ICT systems** means all computer based Information Technology and Communication systems (i.e. hardware and software) and IT related services (user administration, etc.) and their documentation and configuration, which are provided by the council or on their behalf.
Integrity	Integrity of information for the purposes of this context, is the requirement to protect information against tampering with the content, and assurance that it is consistent and correct
Intellectual Property	Intellectual property is the ownership of a set of rights arising from someone's idea, invention, creation, etc., which can be protected by law from being copied.
Government Security Classification Policy	This is a scheme for applying a classification to items of information, permitting different levels of security controls to be applied to management of information with different degrees of sensitivity and privacy. It uses classifications such as "OFFICIAL"". The council Information Handling policy is based on the Government Security Classification policy.
Guidelines	Documents which detail information security best practice and advice.
ISF	Information Security Forum is a body comprising representatives from each Service. Members have responsibilities for co-ordinating implementation of this policy and for assisting in security awareness initiatives within their service areas.
ISO27001	International Standards Organisation 27001 -The standard for Information Security Management
Malicious Code	A piece of hostile programming code designed to interfere with the normal operation of computers and networks, and possibly replicate itself across networks to other connected computers e.g. a virus or worm.
Malware	**Malware**,-short for *malicious software*, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer

	virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.
Mobile Code	Mobile code is code obtained from remote systems, transferred across networks and them downloaded and executed on local systems without explicit installation or execution by the recipient.
Mobile Device	End user device such as laptops, tablets and smartphones
Monitoring	Monitoring is defined as the targeted observation of e-mail and internet use, traffic and content.
Peer-to-Peer File Sharing	Peer-to-Peer (P2P) is software that allows computer users, using the same software, to connect with each other and directly access files from one another's hard drives. There are many security concerns about this type of facility.
Policy	A high level set of regulations or rules which govern people's activities. They are usually based upon an underlying set of principles.
Pop-ups	Pop-ups are windows which automatically open up when you visit some websites. They are often adverts and contain a link to different website.
Procedures	Step by step instructions detailing how policy and standards will be implemented in an operating environment..
Public Network	A public network is a type of network wherein anyone, namely the general public, has access and through it can connect to other networks or the internet. This is in contrast to a private network, where restrictions and access rules are established in order to relegate access to a select few. Since a public network has few or no restrictions, users need to be wary of possible security risks when accessing it.
Sensitive Information	For the purposes of this policy "Sensitive Information" can fall into two categories, personal information and non-personal information. Personal sensitive information is defined and governed by the Data Protection Act. Non-personal sensitive information can be any information which does not relate to any specific identifiable individual but it is still of value to the Council and its circulation and publication requires to be restricted for some reason. This could be commercially–sensitive, financial or operational information which the council would not want in the public domain at a particular point in time as it might prejudice council operations, undermine formal processes or expose the council to some form of operational or reputational risk. When handling information which falls into the above categories great care must be taken to follow the council 's Information Handling policy andnot to expose it outwith those authorised to see it.
Shared Area	This term refers to computer storage systems provided by North Lanarkshire Council to allow employees to carry out their normal duties and include: • Public Drives (I: Drives) • Personal Drives (H: Drives) • Exchange Public Folders • Connect/Website • First Class Conferences • EDRMS -Electronic Document Records Management System.
Smartphones	Electronic handheld device that integrates the functionality of a mobile phone, personal digital assistant (PDA) or other information appliance. As well as all of the standard mobile phone functions, these offer many of the facilities you would find on a personal computer, such as e-mail, internet browsing and mass data storage.
Standards	Mandatory activities, actions, rules or regulations designed to support policies with the specific technical or operational detail required to make them meaningful and effective. The standards are derived from the international security standard for Information Security Management ISO 27001and the BS17799 the British Standard for Information Security Management.
Tablets	Mobile end-user devices including iPads
Third Parties	This term relates to every person who makes use of North Lanarkshire Council ICT systems that is not an employee including but not limited to councillors, contractors, trainees, school pupils and employees of companies providing services on behalf of NLC.
Third Party Links	A third party link is a link on a web site which redirects the user to a different website.

Appendix B: PSN (Public Services Network) and GCSX (Government Connect Secure eXtranet)

The Public Services Network (PSN) is a facility where services, including the Government Connect Secure eXtranet (GCSX), can be shared safely among public bodies. These services include the Blue Badge service, Registration services and email. The email service works on the basis of providing secure e-mail addresses in each member organisation which subscribes to it. Organisations pay an annual per-mailbox fee and a cost per GCSX e-mail message. There are currently more than 1000 GCSX mailboxes in use by the council at a significant cost.

For each organisation to become, and remain, a member of this scheme they have to confirm that the operation of their own networks and systems meets a security standard set by the government body which runs the scheme.

This standard is called the PSN Code of Connection. Any organisation failing to meet the standard will either be refused access to the scheme, or for existing members can have the facility taken away from them. The council, along with all other PSN members, must confirm their compliance with the Code of Connection annually. There are a number of rules surrounding use of PSN for both the organisation and for individual users.

Service managers will decide who in their organisation requires a GCSX mail account. Because PSN is a “closed” system GCSX mail must not be sent to non-PSN mailboxes.

General Rules

- Use of the PSN may be monitored and/or recorded for lawful purposes;
- Each GCSX email user will be held responsible for the use of their GCSX mail account;
- Each GCSX mailbox must have a council employee as accountable owner.
- Access PSN services only from council managed devices.

Specific Rules

Do:

- Treat mail received via PSN with care and take account of the sensitivity of the information received;
- Disclose information received via the PSN only on a ‘need-to-know’ basis;
- Always check that the recipients of e-mail messages are correct so that potentially sensitive information is not accidentally released into the public domain;
- Forward PSN mail (only if there is a need for it and you have the permissions of the sender) via a suitably secure communication channel;
- Carefully check the distribution list for any GCSX mail you are planning to send out;
- Securely store or destroy any material printed from PSN mail.

Do Not:

- Use a GCSX mailbox belonging to a colleague;
- Access any computer system which you have not been given explicit authority to access;
- Access the PSN from systems and locations which have not been expressly authorised for the purpose (e.g. you should not access PSN mail from an internet café);
- Transmit information via the PSN that you know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- Auto-forward e-mail from a GCSX account to any other non-PSN e-mail account;
- Forward or disclose any sensitive or protectively marked material received via the PSN unless you have the permission of the sender and the recipient(s) can be trusted to handle the material securely.

Appendix C: Supporting legislation, policies, standards

Legislation

- Data Protection Act 1998
- Environmental Information (Scotland) Regulations 2004
- Freedom of Information (Scotland) Act 2002
- Information associated aspects of the Human Rights Act 1998
- Information associated aspects of the Local Government in Scotland Act 2003
- INSPIRE (Scotland) regulations 2009

Internal

- Acceptable Use of ICT Policy
- Acceptable Use of ICT Guidelines
- Data Protection Policy
- Flexible Workstyle Handbook
- ICT Security Policy
- Information Security Good Practice Guidelines
- Information Asset Register
- Records Management Plan
- Corporate File Plan
- Information Governance Policy Framework
- Information Risk Policy
- Information Handing Policy
- Records and Information Management Policy
- STD 0125 System Access Password Standard
- Dignity at work Policy
- Discipline Policy
- JNCT Disciplinary Framework for Teachers
- Employee code of conduct
- Time Off for trade union duties guidance note
- Contract standing orders
- Whistleblowing procedure

External

- Codes of practices issued by regulatory and statutory bodies (e.g. Information Commissioner's Office, audit Scotland etc).
- Public Services Network
- ISO 27001 and 27002 Information Security Management Standards
- Lanarkshire Data Information Sharing Partnership
- Payment Card Industry Data Security Standards (PCI DSS) Standards