Staff Acceptable Use Policy

Date: January 2021

Policy Information	
Policy Title	Staff Acceptable Use Policy
Policy Number:	POL 035
Version	5.0
Policy Sponsor	Director of Business Support
Policy Owner	Head of ICU/ICT
Committee and date recommended for approval	Business Support Committee
Date approved by the Board	11 February 2021
Equality Screening Status	Screening Reviewed: 12 January 2021
Rural Needs Impact Assessment Status	Rural needs impact assessed: 12 January 2021
Date Set For Review	January 2024
Related Policies	POL029 Server Security Policy POL030 Network Security Policy POL031 Internet Security Policy POL032 IT Security Policy POL033 Microsoft Windows Client Security Policy POL034 Application Security Policy

1. Introduction

This policy applies to all Libraries NI employees whether full time or part time, seconded staff, temporary staff, agency staff, contractors, consultants, and associates.

The Information Security Manager (Head of ICU/ICT) owns this policy. Any queries regarding the policy content should be directed to the Information Security Manager within Libraries NI.

2. Purpose

The objective of this Acceptable Use Policy is to detail how Libraries NI will manage and monitor the use of its information assets and systems and the standards it requires from its users.

The requirements of this policy apply to all IT systems owned by Libraries NI, administered by Libraries NI, and/or administered on behalf of Libraries NI, whether in the Data Centres, in library locations, or elsewhere. It applies across the entire Libraries NI IT environment.

3. Policy

3.1 Responsibilities

A number of different groups have responsibility within Libraries NI for aspects of IT Security. In particular, the following have specific responsibility for adherence to this standard as outlined below.

IT Help Desk

The IT Help Desk has primary responsibility for the management of user accounts within the Libraries NI environment.

Staff Users

Users of the Libraries NI IT environment are provided with a user account, for the purpose of carrying out their roles and responsibilities within the Libraries NI environment. Each user is responsible for protecting access to their account, and for maintaining the appropriate confidentiality of their data with which they are working. Users must not divulge their account passwords to others, must not permit others to use their accounts, and must not use accounts intended for the sole use of other individuals. Users have responsibilities under the Code of Conduct for Staff Safeguarding Policy and obligations under a legislation including the Data Protection Act 2018.

Users are responsible for escalating security incidents to nominated staff at their Library. Nominated staff are responsible for escalating such incidents to the Information Security Manager for investigation and resolution. Data

protection issues or breaches should be escalated to the Information Security Manager as soon as possible.

Information Security Manager

The Information Security Manager is responsible for security within the day-to-day operation of the Libraries NI environment. This includes security monitoring, and the investigation and resolution of any security incidents that occur. He/she is also responsible for liaising with the Authority over major security incidents, violations of policy, and reviewing and updating the Libraries NI security documentation when required.

3.2 e-Mail Acceptable Use

Users, where appropriate, will be provided with individual email accounts to use for the purpose of Libraries NI business.

The following activities are considered unacceptable use of corporate e-mail:

- ending SPAM or phishing emails
- sending email containing inappropriate, obscene, racist, or insulting language
- sending email that is provocative, suggestive or discriminatory
- sending email that intimidates or harasses the recipient
- sending email that pretends to come from someone else
- sending email and email content containing libraries information
    - (including attachments) to unauthorised users
- using the email service to facilitate or participate in a suspected criminal activity
- sending an e-mail which has an adverse impact on the performance of the network.

In addition, the following activities may constitute unacceptable use, unless specifically authorised or for approved business purposes:

- subscribing to mailing lists.

3.3 Web Browsing Acceptable Use

Users will be permitted to browse the Internet and the service is designed to reduce the risk of access to inappropriate material. However, users must also use the service in an acceptable manner to reduce the risks of accessing such material. The following activities are considered an **unacceptable use** of web browsing services within the Libraries NI IT environment:

- deliberate access to inappropriate material
- downloading and/or installation of software without permission
- any use that could bring Libraries NI into disrepute.

3.4 Social Media

The following activities are considered **unacceptable use** of social media, newsgroups, and bulletin boards:

- participation in discussions of an illegal, obscene, discriminatory or abusive nature
- participation in discussions which are defamatory to Libraries NI and its services or would bring the service into disrepute
- any post (e.g. a Tweet or Facebook status update) that would bring the service into disrepute.

3.5 Memory Sticks and Other Removable Media

The use of memory sticks or other removable media is not permitted by staff to transfer information into and out of the Libraries NI environment

3.6 Web Publishing

The Libraries NI environment provides facilities for publication on the World Wide Web for Library related information. In addition, individual information may be published with the explicit approval of the Library.

The following activities are considered **unacceptable use** of web publishing:

- unauthorised publication of information of a personal nature
- unauthorised publication of information that could lead to identification of an individual
- publication of anything of an illegal, obscene, discriminatory, or abusive nature
- publication of copyright material without the owner's consent
- publication of anything that is likely to mislead others.

In addition, the following activities may constitute unacceptable use, unless specifically authorised:

- publication of any unauthorised contact information
- publication of out of date information.

3.7 Clear Desk and Clear Screen

When leaving a desk unattended it should be cleared of all sensitive media. When leaving a laptop or PC unattended the computer must be locked, which can be achieved through pressing the ***Ctrl+Alt+Del*** keys together and selecting the ***Lock This Computer*** option or Windows key and L. Desktop and Laptop sessions and open sessions on applications should be logged off and, where appropriate, shut down when no longer required or at the end of a working day.

3.8 Considerations for IT Operations Staff

In many cases, ICT staff (both internal and external to Libraries NI) will have access to other users' information and files within the Libraries NI environment. This information must only be accessed for operational purposes. It must never be copied outside the Libraries NI environment without the permission of the owner of the information or file. Inappropriate access to, or misuse of, personal information within the Libraries NI environment will be considered as a serious disciplinary offence.

3.9 Other Unacceptable Use of IT Services

The Information Security Manager can provide guidance on appropriate use of the Internet.

This section does not in any way provide a complete list of usage and behaviours that are considered unacceptable. Instead it gives some examples of unacceptable use in order to help users make decisions on unclear areas.

The following activities will always be considered **unacceptable use** of the Libraries NI environment:

- propagation of chain emails
- development, or deliberate release, of rogue code (i.e. viruses, Trojans, etc.)
- interference with the work of other users (e.g. altering or copying their work)
- grooming
- hacking systems within the Libraries NI environment or on the Internet
- unauthorised access to systems
- actions that bring the Library, or the Libraries NI environment, into disrepute, or that are likely to do so
- deliberately wasting resources (e.g. unnecessary copying or emailing of very large files)
- use of the environment for personal financial gain
- any illegal activity, including breach of copyright
- release of another person's personal information
- any action that is intended to circumvent or disable the security measures in place within the Libraries NI environment.

In addition, the following activities may constitute unacceptable use, unless specifically authorised:

- use of other users' personal accounts
- accessing other users' personal information
- scanning systems within the Libraries NI environment or the Internet
- any use that interferes with, or prevents, another user's permitted use of the environment
- unauthorised modification or reconfiguration of Libraries NI systems, including installation of software.

3.10 What Users May Do

Within this overall context users may (subject to the safeguards and conditions set out in this and any other relevant policy or guidance):

- use e-mail to communicate with colleagues, customers, suppliers and other interested parties in carrying out their Libraries NI duties
- use the Internet to research relevant and potentially relevant information sources in carrying out their duties. In doing so, users may glean relevant information from trusted third parties (including news sites), provided prior approval for such access has been granted by line managers
- participate in newsgroups, chat rooms, or social media websites in the course of business relevant to their duties. When so doing, users must not (unless specifically authorised to do so) speak or write in any Libraries NI name and must make it clear that their participation is as an individual speaking only for themselves. In any such use of Internet/e-mail facilities, users must identify themselves honestly, accurately and completely.

<u>When participating in a chat forum or newsgroup users must:</u>

- refrain from any political advocacy and from the unauthorised endorsement or appearance of endorsement of any commercial product or service
- give due regard to maintaining the clarity, consistency and integrity of Libraries NI corporate image and avoid making any inferences that may prove inappropriate from a Libraries NI perspective.

<u>And must not:</u>

- reveal protectively marked information, customer data, or any other material covered by Libraries NI policies and procedures
- use Libraries NI Internet facilities or computing resources to violate laws and regulations applicable in United Kingdom in any way or to compromise the security (including confidentiality) of Libraries NI data.

3.11 What Users Must Do

At all times users must:

- keep all passwords or user IDs confidential - the sharing of user IDs or passwords is prohibited
- be alert to the risk of leaving an unattended machine logged on, which could lead to unauthorised use of their account and user ID
- follow the security procedures approved for use with their system to ensure that any file downloaded from the Internet is scanned for viruses before it is accessed or run. Users who download such files, or who open attachments to e-mails, are responsible for ensuring that they are subjected to appropriate anti-virus scans (checking with the Fujitsu Service Desk as necessary)
- report immediately any indication of virus or other attack to the Fujitsu Service Desk or ICU
- report immediately to their line manager or, if appropriate, to the Human Resources Manager, the receipt of inappropriate or offensive material delivered via e-mail
- respect copyrights, software licensing rules and property rights
- download only software with direct business use and do so in accordance with relevant Libraries NI policy
- as far as possible, schedule communication-intensive operations such as large file transfers, video downloads, mass e-mailings, etc. for off-peak times.

3.12 What Users Must Not Do

Users must not:

- arrange to auto-forward e-mails from their Libraries NI account to personal e-mail accounts, or from their personal e-mail account to Libraries NI accounts. E-mails received into a Libraries NI account may be forwarded once their contents have been vetted to ensure that the forwarding of the e-mails does not contravene guidance in respect of protectively marked material
- knowingly propagate any virus or programme designed to infiltrate a system (without the user's knowledge) to gather information (e.g. worm, Trojan horse) or other type of malicious program code
- use any Libraries NI facilities to disable or overload any computer system or network, or attempt to disable, defeat or circumvent firewalls or any Libraries NI ICT security facility intended to protect the privacy or security of systems, networks or users
- forward, send or store e-mails or other files containing inappropriate material
- knowingly connect to any Internet site that contains inappropriate material. When such a site is inadvertently accessed, users will immediately disconnect from the site, regardless of whether that site had been previously

deemed acceptable by any screening or rating program. Such inadvertent connections must be reported immediately to the ICU so that appropriate action to bar access to the site can be taken and to safeguard the individual in the event of any subsequent investigation

- use any Libraries NI systems or facilities to commit infractions such as harassment, unauthorised public posting, misappropriation of intellectual property or misuse of Libraries NI assets or resources
- intentionally access, archive, store, distribute, edit, record, or reproduce (on screen, hardcopy or via audio) any kind of inappropriate material on any Libraries NI system
- use Libraries NI facilities to download and/or forward non-business related software or data including music, graphics, videos, text, games, entertainment or pirated software
- use Libraries NI facilities to play internet games or forward chain letters (even in the user's own time)
- use Libraries NI facilities to participate in chat rooms, forums or newsgroups unless this is for business purposes
- upload any software licensed to a department or data owned by a department without the express authorisation of the manager responsible for the software or data
- transfer via the **Internet** (as opposed to the Libraries NI **Intranet**) files containing OFFICIAL Libraries NI data unless the data is first encrypted using a product approved by Libraries NI ICU/ICT. Files containing OFFICIAL material may be transferred via Libraries NI Intranet. However, files containing Libraries NI data with a protective marking higher than OFFICIAL must NOT be transferred electronically. and, remain connected to the Internet while not actively using the resource.

3.13 Personal Use

Definition

Personal use is defined as any use of Internet or e-mail facilities that does not stem from a requirement directly relating to the officer's official duties. Thus accessing a site for research purposes, for example researching social security policy or employment law developments, is official use only if such access is necessary as part of the officer's work. Accessing such data only out of personal interest, or to broaden general knowledge in that area, would be classed as personal use if the information is not actually required to discharge duties effectively.

Any access or use which is unrelated to official duties, for example, accessing general news sites, travel information, personal banking, sending or receiving personal e-mails and so on, would be classed as personal use.

Guidance on Personal Use

Libraries NI permits staff to use official facilities for personal use, in their own time, providing that such use does not compromise the security of official data, result in increased costs or delays or have any negative impact on the Libraries NI network or on the effective discharge of official business. Own time is when an individual is not on duty, such as before signing in or after signing out or during lunch or other officially sanctioned breaks. The facility is granted at the discretion of management and may be withdrawn at any time for operational reasons, or if misuse is suspected or detected.

Users are reminded that all Internet and e-mail use is subject to monitoring. Such monitoring does not differentiate between official and personal use. Users should therefore ensure that anyone who may send personal e-mails, or other material, to their official e-mail address is aware that the content of such emails may be monitored. Use of Libraries NI facilities for personal use will be deemed as acceptance that usage, and on occasions, content, will be monitored.

Subject to Libraries NI policies in relation to personal use, users may in their own time:

- use the Internet for the occasional purchase of goods and services, for example, books, flights, CDs, and so on, provided payment is made by the individual, and delivery of items purchased is to a private address. The user must not create any unauthorised contractual liability on the part of Libraries NI. Libraries NI does not accept any responsibility for the security of credit card details, or any other payment method used. Libraries NI does not accept any liability for financial loss, whether as a result of fraud or otherwise, suffered while using Libraries NI systems for personal transactions. All such use is entirely at the individual's own risk
- make occasional use of Libraries NI facilities for on-line banking. All such use will be at the individuals own risk - Libraries NI cannot accept any liability for losses or for any other liabilities arising out of such transactions, howsoever caused
- make occasional use of Libraries NI e-mail accounts set up on their behalf, to send, forward or receive personal e-mails - subject to the conditions for using e-mail facilities set out in this policy. Personal emails must be clearly marked as being "personal". It is an explicit condition of using this facility that users accept that the content of such e-mails may be accessed, by management and/or Corporate ICT staff, without notice or any requirement for further consent. While it is not intended to undertake routine monitoring of the contents of e-mails (personal or otherwise), e-mail traffic may be accessed at any time either as a result of checking an officer's e-mail account for business reasons if they are absent from work, or as part of an exercise to monitor compliance with internet and e-mail usage policy.

Users must not make excessive use of any of the above facilities to the detriment of their official duties.

Restrictions on Personal Use

Users must not:

- use Libraries NI Internet or e-mail facilities to carry out any activities for personal gain including, for example, share dealing or monitoring, investment portfolio management, or gambling.

4. Monitoring

Internet and email use will be subject to monitoring, therefore users should have no expectation of privacy in relation to personal use. Activities identified as being deemed unacceptable or violations of security policies may be subject to disciplinary action. Refer to section 7 Violations for further information.

5. Waivers

Any request for a waiver under this standard should be address to the Information Security Manager. The detail of the waiver should be described, along with a justification that explains why the policy cannot be adhered to, and an outline plan to bring the application or system into compliance in the future. The Information Security Manager will discuss waiver requests with IT Operations and with the Authority, as appropriate.

Waivers can be granted by the Information Security Manager (Head of ICU/ICT) for a period not exceeding one year, but may be extended annually if the justification still applies.

6. Document Review

This document should be reviewed, and updated if necessary, not more than two years from its date of issue. The review will be carried out by the Information Security Manager, and he/she may then recommend updates if necessary. Updates will be presented to the Authority by the Information Security Manager for approval.

7. Violations

Any violations of this security policy should be brought to the attention of the Information Security Manager who will work with the appropriate individuals to rectify the problem.

Persistent violation of this security policy by a member of Library staff may lead to disciplinary proceedings and/or legal proceedings against that individual by the appropriate employing authority.

Persistent violation of this security standard by contract staff, or by staff of third parties in a contractual relationship with Libraries NI, will be treated as a breach of the appropriate contract.

Where a user is involved in persistent violation of this policy, appropriate action will be taken by the User's line manager, or appropriate management representative.

Glossary

Bulletin Board	An Internet-based message board.
Chain email	An email message that requests the recipient to forward it to other people.
Chat room	A system on the Internet that allows users to exchange synchronous remarks.
Grooming	The criminal offence of building a relationship with a child for the purpose of illegal sexual relations.
Hacking	Unauthorised access to a computer system, generally by subverting system login measures.
Mailing List	A list of email addresses to which targeted information is emailed on a regular basis.
Newsgroup	Internet discussion group.
Personal Information	Information pertaining to an individual and identifiable with that individual. Personal information is covered by the UK Data Protection Act.
Rogue code	Any software that is intended to carry out modification, reconfiguration or disruption of, or access to, a computer without the owner's permission. A general term for worms, viruses, Trojans.
Scanning	Repeated access to one system, or access to large numbers of systems, for the purpose of determining the services running, and/or the configuration of the systems.
Social Media	This refers to websites that allow public broadcasting of personal opinion that may be attributed to or reflect on Libraries NI. This includes (but is not limited to) website like Twitter, Facebook, or LinkedIn.
SPAM	Unsolicited email, usually containing advertising.
Trojan	A program that carries out a hidden function while performing a normal, visible service.
Virus	Code that attaches itself to an existing program, and which spreads by infecting other programs when it runs.
Waiver	The process by which a system is permitted to remain in violation of one or more points of a standard.
Worm	Rogue code, like a virus, but which runs on its own instead of attached to another program. Worms also replicate when they run.