Health and Social Care

Northern Ireland Fire & Rescue Service

Information Security

1.03 Use of Internet Services

All User Standard

Approval

Document Reference	Information Security 1.03 – Use of the Internet - All User Standard
Version	0.3
Last updated	1st March 2021
Owner	
Approval by	

Contents

1. INTRODUCTION

Health and Social Care (HSC) and Northern Ireland Fire and Rescue Service (NIFRS) (herein HSC will refer to all HSC and NIFRS organisations) Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

The internet is a global interconnected computer network allowing the majority of our digital devices and systems to communicate with one another, this allows us to access the world wide web, and share data with anyone in the world almost instantly. These uses of the internet are herein referred to as Internet Services. This level of interconnectedness has inherent risks, such as unauthorised individuals trying to gain access to systems that they don't have access to (hackers), malicious software (malware) that can infect our ICT systems and cause disruption to our organisations and social engineering enabled by the internet that can harm our people.

HSC Organisations need to understand these risks and ensure they take the right steps to protect HSC's people, Information Assets and Systems.

2. PURPOSE

This Information Security Standard is in place to ensure HSC and NIFRS organisations are able to use Internet Services in a manner that is effective for the business need, whilst reducing the risk of any losses related to the Confidentiality, Availability or Integrity of HSC or NIFRS Information Assets and Systems.

3. SCOPE

The Information Security Standard applies to:

- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC and NIFRS [1], including:
    - HSC and NIFRS employees
    - Temporary Staff including agency and students
    - Voluntary Health Sector organisations / Volunteers
    - Third Party Contractors
    - Any other party making use of HSC ICT resources
- HSC information stored, or in use, on HSC or externally hosted systems;
- Information in transit across the HSC networks;
- Information leaving HSC networks; and
- ICT Systems belonging to or under the control of HSC.

[1] Northern Ireland Health & Social Care organisations include Health & Social Care Board (HSCB), Public Health Agency (PHA), Health & Social Care Trusts, NI Ambulance Service (NIAS), Business Services Organisation (BSO), Patient & Client Council (PCC), Regulation & Quality Improvement Authority (RQIA), NI Guardian Ad Litem Agency (NIGALA), NI Blood Transfusion Service (NIBTS), NI Social Care Council (NISCC), NI Practice and Education Council for Nursing and Midwifery (NIPEC), NI Medical and Dental Training Agency (NIMDTA), GP Practices and other Independent Contractors to HSC, Northern Ireland Fire and Rescue Service (NIFRS).

This Standard applies throughout the entire information lifecycle from acquisition/creation through utilisation to storage and disposal.

4. STANDARD NON-COMPLIANCE / BREACH

See the Information Security Policy for details of what to do in the event of non-compliance or a breach of an Information Security Standard. For an information Security Breach or Incident, see the Information Security Incident Identification and Reporting All User Standard.

5. USE OF INTERNET SERVICES

Connecting to the HSC Network

5.1.1. Where connection to the internet is required, all staff must connect HSC devices to the HSCNI network regularly to ensure information security controls, such as anti-malware software, are kept up to date.

5.1.2. Any out-of-date information security controls, that have not been able to automatically update, must be reported to the local ICT Service Desk.

5.1.3. A HSC device that has not been connected to the network for 3 months must be disabled from accessing HSCN resources. It may be reenabled upon the user contacting the ICT helpdesk who will ensure security controls are up to date.

Usage of Internet Services

5.1.4. All staff must use internet services in a secure, ethical and legal manner. Staff shall only use internet services for reasonable personal use as agreed with your line manager. Examples of prohibited Internet Services include but are not limited to:

- Attempts to gain unauthorised access to information resources;
- Accessing material that is pornographic, illegal, offensive, or discriminatory;
- Accessing non-approved file sharing services or software;
- Activities that could be damaging to the reputation of the organisation;
- Activities that interfere with business requirements; and
- Activities that violate copyright, license agreements or other contracts.
- The use of proxy avoidance

5.1.5. If access to a blocked internet service is required, staff shall follow their local ICT process to request access. Such access may be denied if a sufficient business reason is not provided, it is a prohibited use, or is deemed a significant risk.

5.1.6. Registering to internet services with a business email address is limited to business only and should not be used for any non-business use such as for personal items. For example online shopping accounts and personal social media.

5.1.7. All personnel shall comply with the Information Security Data Transfer Standard when using Internet Services to transfer HSC information assets.

5.1.8. If there is a business requirement to purchase online goods or internet services, this must be done in accordance with the organisation's local procurement and approval process.

Social Networking and Blog Sites

5.1.9. Staff should follow their local organisations Social Media Policy. Examples of inappropriate use include, but are not limited to:

- Using HSC or any other organisation's brand on social media as their own;
- Using social media to the extent that it interferes with your responsibilities at HSC; and
- Using social media in a way that could be damaging to the reputation of HSC.

Involvement in Forums / User groups

5.1.10. Involvement in Forums / User Groups is permitted for business purposes only and must be authorised by your organisation. Any request for access to any of these forums should have approval of the respective Assistant Director/Director. When so doing, staff must not (unless specifically authorised to do so) speak or write in your organisation's name and must make it clear that their participation is as an individual speaking only for themselves and any comments are their personal opinion. In any such use of internet facilities, employees must identify themselves, with their own full name, honestly, accurately and completely. The misuse of such facilities may lead to disciplinary action when staff are acting in a personal capacity or even in a business capacity.

When participating in a forum / user group, staff **must**:-

- Refrain from 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 the HSC corporate image and avoid making any inferences that may prove inappropriate from a HSC perspective;

and **must not**:

- reveal sensitively marked information, client data, or any other material covered by HSC policies and procedures;
- Use HSC internet facilities or computing resources to violate applicable laws and regulations in any way or to compromise the security (including confidentiality) of HSC data.

Malware and Viruses

5.1.11. All staff should take all reasonable steps to ensure they are not responsible for the introduction of malware or unauthorised access to HSCN or HSC Information Systems. This includes, but is not limited to:

- Not opening files from unknown sources;
- Not downloading software from unapproved sources;
- Taking care when browsing the world wide web, such as using search engines results and visiting unfamiliar websites;
- Not entering HSC identification or authentication information to non-HSC managed Internet Services; and
- Not uploading HSC information to third party websites unless it is part of a contractual agreement with the third party, for example using a third-party online translation service to translate personal information where we do not have a direct and contractual relationship.

Inappropriate Material

5.1.12. Inappropriate material may include, but is not limited to, any material of a pornographic, sexist, racist, sectarian, violent or offensive nature; whether in pictures, cartoons, words, sounds or moving images, whether or not purporting to be of a humorous nature. Staff should be aware that the decision as to what material is considered offensive can depend on the perception of the recipient and/or observer, rather than the intention of the sender. The final decision on what is offensive is determined by the local Director of Human Resources.

When a site containing inappropriate material is accessed, staff must immediately disconnect from the site, regardless of whether that site had been previously deemed acceptable by any screening or rating program. Such connections must be reported immediately to the **Local** Service Desk 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.

Staff should be aware that where attempted access to a website categorised by the Internet Watch Foundation (IWF), e.g. child sexual abuse and criminal matters, is logged the BSO ITS will fully co-operate with the Police Service Northern Ireland (PSNI) to identify and take action against any employee.

All individual employees have a requirement to inform the PSNI immediately should they witness anyone accessing website material which may be categorised by the Internet Watch Foundation. These broadly include:-

- Images of child sexual abuse;
- Criminally obscene content;
- Incitement to racial hatred content.

6. LIABILITY

6.1.1. The HSC does not accept any liability that may arise from employees using the Internet for personal use e.g. personal use of the internet to complete an online transaction, which may at a later stage result in fraud.

Staff should be aware that they might be personally liable to prosecution and open to claims for damages, should their actions be found to be in breach of the law. In cases of harassment, a claim by a person that he/she had not intended to harass or cause offence will not in itself constitute an acceptable defence.

7. MONITORING

7.1.1. Staff must be aware that any data on the organisation's systems remains the property of HSC. HSC reserves the right to monitor and record any use of organisation information and systems to ensure they are used for legitimate purposes, and that policies and standards are being complied with.

7.1.2. All monitoring must be undertaken in accordance with the appropriate legislation such as Regulation of Investigatory Powers Act (2000), Human Rights Act (1998), and good practice guidance such as "Employment Practices Code Part 3: Monitoring at Work" issued by Information Commissioners Office.

8. REVIEW CYCLE

8.1.1. This Standard will be subject to annual review or following any significant incidents, changes to UK or EU legislation or changes to the HSC structure or functional responsibilities.

8.1.2. All HSC organisations are responsible for ensuring their own local Security Policies, Standards, Procedures and Guidance are subject to regular review and take into account any changes to the HSC Information Security Policy and Standards.

<<Add Name>>.

<<Add Role>> Date:

<<Add Name>>.

<<Add Role>> Date: