Health and Social Care

Northern Ireland Fire & Rescue Service

Information Security

1.01 Email Communications All User Standard

Approval

Document Reference	Information Security 1.01 - Email Communications - 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 HSC email system is a significant business, information and communication tool, yet email also poses a significant risk to Information Security. The sensitive nature of the communications sent via email and the high usage of email, mixed with the high likelihood of error and malicious use of email mean that data breaches are likely and could result in harm to individuals, and subsequent regulatory actions being taken against HSC.

2. PURPOSE

This Information Security Standard is in place to ensure HSC and NIFRS organisations are able to use their email 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 or 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;
- ICT Systems belonging to or under the control of HSC.

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

[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, and Northern Ireland Fire and Rescue Service (NIFRS).

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. EMAIL COMMUNICATIONS

5.1. EMAIL USAGE

5.1.1. All staff shall exercise good judgement and use the email system in an acceptable manner and in accordance with all relevant Policies and Standards. Examples of prohibited uses include but are not limited to:

- Transmitting confidential or organisation information to unauthorised individuals;
- Transmitting material that is illegal, offensive or discriminatory;
- Transmitting any material or communication that could be construed as harassment;
- Transmitting spam or malicious content (viruses, spyware, malware);
- Violating copyright, license agreements or other contracts;
- Representing personal opinions as that of the organisation; and
- Forwarding any organisation or client information to personal email addresses.

5.1.2. Personal use (any access which is unrelated to official duties) of HSC email services is only permitted in accordance with local security policies. Personal use of HSC email shall be avoided where possible. Access is not permitted for commercial use.

5.1.3. Emails originating from the HSC email service shall have an automatically applied disclaimer appended to the body of the email. The disclaimer shall provide information such as:

- The Confidentiality / data classification that should be applied to the communication;
- Intended Recipient use only, and direction for where mis-transmission occurs;
- Views and opinions are those of the author, and not necessarily those of HSC;
- HSC Network monitoring may take place to ensure compliance with HSC Policies;
- HSC scans outgoing email, but takes no responsibility for malicious email content; and
- Potential Public disclosure of email communications under the Freedom of Information Act 2000 and GDPR legislation.

5.1.4. All staff are responsible for ensuring the confidentiality of information they send by email.

5.1.5. All personnel shall comply with the Information Security Data Transfer Standard when using email to transfer HSC information to others.

5.1.6. Personal data must not be sent by email outside the HSC network unless following

agreed and documented processes that include the appropriate security measures, and as approved by the HSC ICT department such as file encryption or cloud based secure transfer services.

5.1.7. HSC Information Assets, including personally identifiable information, must not be emailed either to or from any staff member's personal email account.

5.1.8. All Staff must not arrange to auto-forward emails from their HSC account to other e-mail accounts e.g. @doctors.org @qub.ac.uk, or from their personal e-mail accounts to their HSC account.

Your HSC email account will contain sensitive information and that must be vetted before being forwarded on to any other email account. Auto-forwarding removes this vetting stage.

5.1.9. Refer to the local policy for details on email retention periods and maximum mail box sizes.

5.2. PHISHING AND SOCIAL ENGINEERING

5.2.1. All staff shall be trained to identify phishing or social engineering email communications.

5.2.2. All staff must not interact with suspected or actual phishing / social engineering communications. If unsure of the validity of an email or any other communication, seek guidance from the local ICT Service Desk.

5.2.3. Particular attention must be given to emails, especially containing attachments, links or files, from unknown or dubious sources. Where there is doubt or suspicion, advice should be sought from the local ICT Service Desk before any such email is opened.

5.3. ACCESS TO ANOTHER INDIVIDUAL'S MAILBOX

5.3.1. Unauthorised access to other user's E-mail accounts and mailbox is forbidden.

5.3.2. Where staff take periods of scheduled leave e.g. annual leave, term time etc. and there is a need to access historical emails, they should grant permission to the appropriate people. Guidance on how to do this is available from your local organisation IT Helpdesk.

If there is a business need to access another user's mailbox in circumstances such as sick leave or personal emergencies were an absence from work is unexpected, the request may be granted to the appropriate line manager. The line manager will firstly take reasonable steps to notify the employee that access is being requested for business reasons. This step is to inform the owner of the mailbox, not seek permission from them. Human Resources have approved view only access via this process and it is restricted to business related emails. Staff should note that it is not technically possible to prevent access to specific emails, e.g. personal ones, held within a mailbox where delegate access has been granted. Where these emails have to be retained moving them to a specific folder labelled Personal and or clearly marking them in the subject line as Personal should be considered.

When the employee returns, the authorising manager will inform the employee that their email account had been accessed by other individuals and the reason why this was necessary.

6. LIABILITY

6.1.1. The HSC does not accept any liability that may arise from employees using hscni.net email for personal use e.g. personal use of the email in response to spam, 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.

Staff are further reminded that under Section 77 of the Freedom of Information Act 2000 it is a criminal offence after a request for information has been received under the Act to alter, deface, block, erase, destroy or conceal any record held by the HSC, with the intention of preventing the disclosure by the HSC of all, or any part, of the information to the communication of which the applicant would have been entitled. This clearly includes any E-Mail related to the request.

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: