HSC Business Services Organisation

Title	**BSO Use of Electronic Mail**

Summary	The policy is to be followed when using the BSO email service.
Purpose	It outlines the permissible use of business email when accessing services from the workplace or using HSC resources remotely (e.g. laptop connected to HSC VPN remote access service).
Operational date	2 January 2016
Review date	2 January 2018
Version Number	V2.0
Supersedes previous	V1.4
Director responsible	Director of Customer Care and Performance
Lead author	Michael Harnett
Lead author, position	Security Operations Manager
Additional authors	David Cassidy
Department	BSO ITS
Contact details	michael.harnett@hscni.net Tel: 028 9536 2279
Equality Screened	Yes

Reference number	
Supersedes	1.4

Version Control

Date	Version	Author	Comments
01.04.2010	1.0	Michael Harnett	BSO Board approved
27.04.2010	1.0.1	Michael Harnett	BSO policy template applied
29.10.2010	1.0.2	Michael Harnett	Wording of Email disclaimer amended.
13.03.2012	1.0.3	David Cassidy	Minor Updates
31.10.2012	1.1	Michael Harnett	Minor Updates
27.07.2015	1.2	Michael Harnett	Minor Updates
23.11.2015	1.3	Scott Stevenson	Addition to Para 14 by SMT
01.12.2015	1.4	Michael Harnett	Added section on Out of Office message
17.12.2015	2.0	Michael Harnett	BSO Board approved

Policy Record

		Date	Version
Author(s)			
Director responsible			

Approval Process

Senior Management Team			
Chief Executive			

CONTENT

1. PURPOSE

This Use of Electronic Mail Policy outlines the permissible use of business email when accessing services from the workplace or using HSC resources remotely (e.g. laptop connected to HSC Checkpoint secure remote access service).

This policy applies to **all staff**, including regular full-time, regular part-time, contractors, consultants, agency and temporary employees.

2. GENERAL USE

Email is a corporate communication business tool, and email communications must be used in a suitable professional manner, appropriate to the organisation and working of the team.

To prevent unauthorised access to your email from your workstation, you must ensure that it is secured (i.e. locked) while you are away from the keyboard.

The provisions of the Data Protection Act 1998 (and any related legislation), the Freedom of Information Act 2000 and the organisation's policies and procedures relating to Data Protection, Freedom of Information and Confidentiality also apply to email communications and the content of those communications. This means that emails may be disclosed to individuals or outside agencies, as required by current Data Protection and Freedom of Information legislation or as required by any other statutory or legal duty imposed on the organisation.

An appropriate subject heading should be used for each email in line with records management arrangements.

3. PERSONAL USE

Personal use of email is permitted subject to the terms of this policy. Such personal use is restricted to staff free time and must be kept to reasonable levels. Staff are also instructed to include the disclaimer below in all personal e-mail:

> "This e-mail is a personal communication and is not authorised by or sent on behalf of any other person or organisation"

Staff **must** not register their hscni.net mailbox with websites for personal use e.g. Amazon, Groupon. Private email accounts should be used in these cases as use of hscni.net mailboxes could potentially increase the amount of spam sent to the HSC. Where a member of staff has already registered their hscni.net account they should take steps to remove this immediately.

Where identified, mailshots will be blocked and not forwarded to hscni.net mailboxes, e.g. Amazon, Easyjet and Groupon offers.

Staff should permanently delete personal emails as soon as possible. This includes the Inbox, Sent Items and Deleted Items.

Abuse of the personal use of e-mail privilege may result in its withdrawal and possible disciplinary action against the staff concerned.

4. PROHIBITED USE

The E-Mail system must **NOT** be used to:

- Transmit pornographic, obscene, offensive, illegal or damaging material. Staff must not take deliberate steps to receive pornographic, obscene, offensive, illegal or damaging material;
- Transmit threatening material or material intended to frighten, harass or bully;
- Transmit defamatory material;
- Infringe copyright;
- Forward chain messages, jokes or images;
- Transmit unsolicited advertising or similar activities i.e. spamming;
- For personal monetary gain or for commercial purposes that are not directly related to HSC business;
- Harass or intimidate others or to interfere with the ability of others to conduct HSC business.
- Attempt unauthorised access to other networks or systems.
- Introduce viruses, spyware or malware onto HSC equipment or network;
- Represent personal opinions as that of the organisation;
- Illegally distribute any personal identifiable or business sensitive material;
- Unauthorised access to other users' e-mail accounts is prohibited;
- Attempting unauthorised access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorisation is a breach of policy.

5. SENDING SENSITIVE / PERSONAL INFORMATION

At present there is not a requirement to apply encryption to sensitive information stored in HSC premises or transferred across the HSC network to other HSC organisations within Northern Ireland. Information transferred between the HSCB, Trusts and Northern Ireland Department of Health is not sent across the internet, If you are transferring information to any addressed that does not end in one of those listed below, it is essential that electronic measures to secure the data in transit, are employed, and it is advised that encryption is therefore applied at all times to transfers of sensitive / personal information.

List of email address domains **within the Northern Ireland private network**

'.hscni.net',

‘n-i.nhs.uk’
‘ni.gov.uk’ or
‘.ni.gov.net’

No sensitive or patient data must be emailed to an address other than those listed above unless they have been protected by encryption mechanisms that have been approved by the BSO ITS.

Where sensitive or patient information has to be sent externally, a number of additional mail services are available:

- BSO Secure Mail Service
- Criminal Justice Secure Mail Service

Note: It is important to remember that although there is a degree of protection afforded to email traffic that contains sensitive information when transmitting within the Northern Ireland HSC network that it is important that the information is sent to the correct recipient. With the amalgamation of many email systems, the chances of a name being the same or similar to the intended recipient has increased. It is therefore recommended that the following simple mechanism is employed when transmitting information to a new contact or to an officer you have not emailed previously.

Step 1. Contact the recipient and ask for their email address.

Step 2. Send a test email to the address provided to ensure that you have inserted the correct email address.

Step 3. Ask the recipient on receiving the test email to reply confirming receipt.

Step 4. Attach the information to be sent with a subject line ‘Private and Confidential, Addressee Only’ to the confirmation receipt email and send.

More information on these services is available on the BSO Intranet site Alternatively you should contact the HSC ICT Security Manager.

Examples of sensitive and personal information include but are not limited to:-

- copies or extracts of data from clinical systems;
- commercially sensitive information;
- contracts under consideration;
- budgets;
- staff reports;
- appointments – actual or potential not yet announced;
- disciplinary or criminal investigations.

Personal data is further defined by the Data Protection Act (1998).

When sending sensitive data, it is recommended that the J-Zip encryption tool or Microsoft Word’s encryption function should be used. It enables information to be encrypted to suitable level for sending through less secure mail systems.

Information on where to locate the software and a guide on how it is used can be found on the BSO Intranet site.

A delivery receipt should be requested with all email containing sensitive / personal data.

6. SPAM / PHISHING

Spam e-mail is also known as ‘junk’ or ‘bulk’ email which is sent to millions of e-mail addresses every single day. The messages usually contain information on purchasing such things as prescription drugs, holidays and financial services.

Phishing is the process of attempting to acquire details from users such as usernames, passwords and banking details i.e. account numbers or credit card information by masquerading as a trustworthy source. This is done by presenting people with emails that look legitimate but direct users to sites that are not.

Spam and Phishing filters are in place and capture the vast majority of this traffic. However they cannot guarantee 100% success. New spam and phishing assaults are developed everyday so the filters have to react to them in the same way the anti-virus vendors operate.

Therefore:-

- Particular attention must be given to emails, especially containing attachments or zip files, from unknown or dubious sources. Where there is doubt or suspicion, advice should be sought from the HSC ICT Security Manager before any such email is opened;

- Seeking information by deception is increasingly being used to gain access to sensitive and personal information. Staff must never respond to email requests from unknown or external sources asking them to divulge personal information or sensitive corporate information; Any such attempt to do so should be brought to the attention of your immediate superior and the HSC ICT Security Manager;

- In order to ensure appropriate corrective action is taken, and no unnecessary panic is caused by hoaxes, staff must report any virus incidents immediately or any other apparent breach in security, to the HSC ICT Security Manager. It is recommended that staff should not take it upon themselves to issue warnings to staff within or outside this organisation;

- If staff receive an e-mail they believe to be a phishing scam, they should contact the HSC ICT Security Manager (ictsecuritymanager@hscni.net) and forward the email for further investigation;

- Where possible never open and definitely never reply to any SPAM or Phishing emails.

To prevent suspect or inappropriate mail from entering the BSO mail system, a quarantine system has been put into place. Further information and details on how to access a legitimate work related email that has been quarantined, can be found in the BSO 'Email Quarantine Service - User Guide', a copy of which is available on the BSO intranet site.

7. ATTACHMENTS

Large attachments (> 20 Mb), unless it is essential that they are delivered urgently, should not be sent between 09.00 and 17.00 on normal working days as network performance can be degraded as a result. The BSOITS Technical Operations Team must be informed beforehand, giving details of the intended recipient and the file size of the attachment, where such transfers are necessary within those hours.

The sending of executable files (.exe), images, movie and music files using the HSC email system, unless they are for business purposes, is strictly prohibited.

8. EMAIL DISCLAIMER

Staff should note that an email disclaimer will be automatically added to any email sent to a non HSCNI address. This is split into 2 parts:

- A strapline at the head of the email content stating

"This email is covered by the disclaimer found at the end of the message."

- The disclaimer at the foot of the email content stating

“The information contained in this email and any attachments is confidential and intended solely for the attention and use of the named addressee(s). No confidentiality or privilege is waived or lost by any mistransmission. If you are not the intended recipient of this email, please inform the sender by return email and destroy all copies. Any views or opinions presented are solely those of the author and do not necessarily represent the views of this Health Social Care (HSC) body. The content of emails sent and received via the HSC network may be monitored for the purposes of ensuring compliance with HSC policies and procedures. While the HSC takes precautions in scanning outgoing emails for computer viruses, no responsibility will be accepted by this HSC body in the event that the email is infected by a computer virus. All emails held by this HSC body may be subject to public disclosure under the Freedom of Information Act 2000.”

9. EMAIL SIGNATURE

Below is a suggested layout for the Insert Signature function available on the email client.

Name:	Xxxxxxx Xxxxxx
Role:	Xxxxxxx Xxxxxx
Tel:	028 12345678
Mobile:	If applicable
Fax:	028 12345678

This signature must not contain any animation, images of your actual signature or graphics unless approved by the HSC ICT Security Manager. This will reduce the storage space needed by the mail server.

The use of background graphics/images is also prohibited to reduce storage space in the mail servers.

10. OUT OF OFFICE MESSAGE

Where staff are out of the office and unable to respond to email for extended periods an auto-reply message should be enabled for your incoming emails. This will notify senders when you are available to respond to their emails.

Example text

> *Thank you for your email. I am out of the office from [DAY, DATE] to [DAY, DATE] and unable to respond at this time.*
>
> *I will review your message following my return on [DAY, DATE]. If you need immediate assistance, contact [Name, phone number and email address].*
>
> *Thank you for your understanding.*
> *Best regards,*
> *Your Name*

If you have access via a corporate Blackberry and will be occasionally reviewing your email then you could change the wording to
Thank you for your email. I am out of the office from [DAY, DATE] to [DAY, DATE] and only have limited access to email.

11. ACCESS TO ANOTHER INDIVIDUAL’S MAILBOX

Where staff take periods of scheduled leave e.g. annual leave, term time etc. and there is a need to access historical emails, then they should grant permission to the appropriate people. Guidance on how to do this is available on the BSO intranet web site.

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 BSO 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.

12. AUTOMATIC EMAIL FORWARDING

Users must not arrange to auto-forward emails from their HSC account to personal e-mail accounts e.g. Gmail and Yahoo! Mail, 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.

13. MONITORING

Users of ICT resources, including the business email, should be aware and must accept as a condition of use that their usage of such facilities will be monitored and may be reviewed whether use is for the conduct of official business or for personal use.

Staff should note that, as is permitted by legislation, business email accounts will be monitored to ensure:-

- compliance to this policy;
- protection of the HSC from liabilities such as harassment and discrimination in the workplace, defamation, and the unauthorised or unnecessary transmitting of confidential information;
- guarding against inappropriate and excessive personal use.

Staff should be aware that any official business conducted using private email accounts (such as Hotmail, Yahoo! Or Gmail) is disclosable under Section 3(2)(b) of the Freedom of Information Act 2000 (FOIA)

Any failure to comply with an FOI request, involving your private email account may be reported to the Information Commissioner’s Office.

Staff should also note that attempts to conceal or delete this information with the intention of preventing its disclosure following receipt of a request is a criminal offence under section 77 of Freedom Of Information Act leaving them personally liable to prosecution. Breaches of the law carry a fine up to £5,000.

14. NON-COMPLIANCE

Any breach of this policy can result in disciplinary action being initiated which may result in dismissal.

Non-compliance can also damage the reputation of the HSC and open the HSC and the individual to a host of legal liabilities

15. LIABILITY

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 BSO, with the intention of preventing the disclosure by the BSO 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.