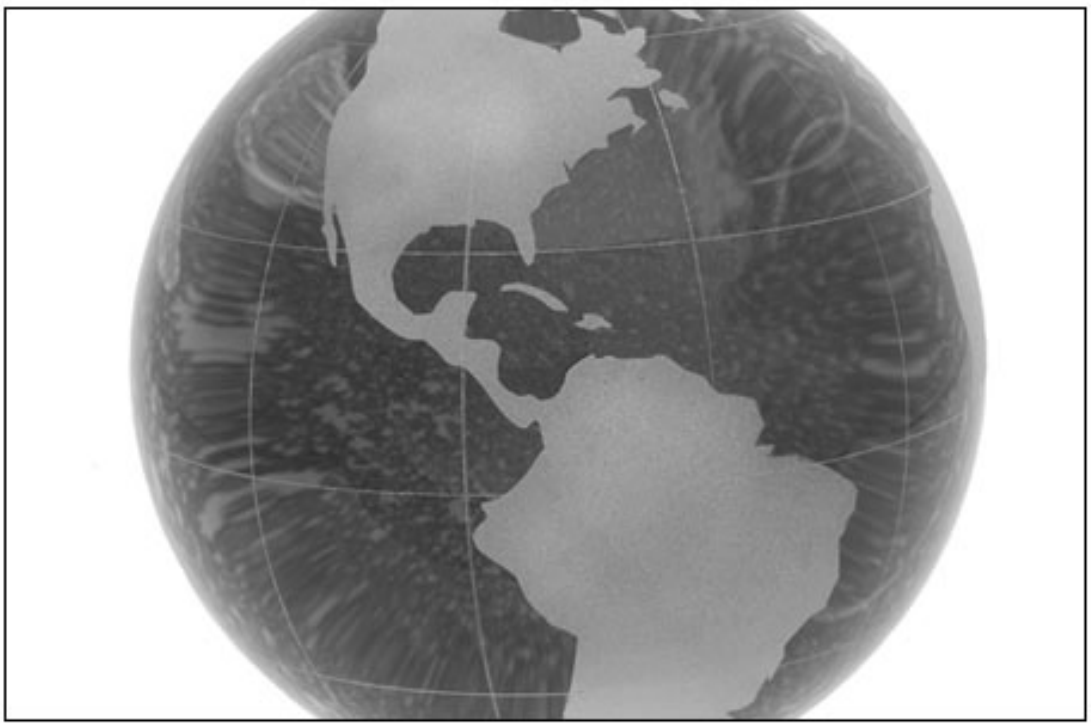
Business Services Organisation

BSO USE OF ELECTRONIC MAIL

(version 1.0)



Approved at BSO Board on 25th February 2010

CONTENT

1. PURPOSE

1.1 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 VPN remote access service).

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

2. GENERAL USE

2.1 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.

2.2 To prevent unauthorised access to a user's email from their workstation, they must ensure that is secure (i.e. locked) while they are away from the keyboard.

2.3 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 communication. 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.

2.4 An appropriate subject heading should be used for each email.

3. PERSONAL USE

3.1 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"

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

3.3 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

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

- Transmit 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 or jokes;
- 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

5.1 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. However it is recommended that encryption is applied at all times to transfers of sensitive / personal information.

5.2 Emails destined for addresses **NOT** ending in

'.hscni.net',
'.nhs.uk' or
'.gov.uk'

will be transmitted across the internet. Therefore **no sensitive or patient data** may be emailed to such addresses unless they have been protected by encryption mechanisms that have been approved by the BSO-ITS.

5.3 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.

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

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

6. SPAM / PHISHING

6.1 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.

6.2 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.

6.3 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.

6.4 Therefore:-

- Particular attention must be given to emails 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;

- Users must never respond to email requests asking them to divulge personal information;

- 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.

7. ATTACHMENTS

7.1 Large attachments (> 10 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 BSO-ITS Email 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.

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

8. EMAIL DISCLAIMER

8.1 An email disclaimer will be added to all messages. Below is an example of one.

****
The information contained in this email and any attachments may contain confidential, proprietary or legally privileged information and is intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent the views of the organisation it was sent from. No confidentiality or privilege is waived or lost by any errors in transmission. If you receive this message in error, please immediately delete it and all copies of it from your system, destroy any hard copies of it and notify the sender. You must not, directly or indirectly, use, disclose, distribute, print, or copy any part of this message if you are not the intended recipient.

The contents of this e-mail and any attachments or replies may be subject to public disclosure under Freedom of Information Act 2000, unless legally exempt. Health and Social Care for Northern Ireland may monitor the content of e-mails sent and received via its network for the purposes of ensuring compliance with its policies and procedures. By opening this email and sending replies you consent to such monitoring taking place. Health and Social Care for Northern Ireland take precautions in scanning outgoing emails for computer viruses using anti-virus software; however it is the recipient's responsibility to take their own precautions in relation to virus scanning.
****

9. EMAIL SIGNATURE

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

Name: Xxxxxx Xxxxxx
Role: Xxxxxx Xxxxxx

Tel: 028 12345678
Mobile: If applicable
Fax: 028 12345678

9.2 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.

9.3 The use of backgrounds is also prohibited to reduce storage space in the mail servers.

10. ACCESS TO ANOTHER INDIVIDUAL'S MAILBOX

10.1 Where staff take periods of scheduled leave e.g. annual leave, term time etc. and there is a need to access to 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.

10.2 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.

10.3 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.

10.4 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 were 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.

10.4 When the employee returns, the ICT Security Officer will inform the employee at their email account had been accessed by other individuals and the reason why.

11. AUTOMATIC EMAIL FORWARDING

11.1 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.

11.2 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.

12. MONITORING

12.1 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.

12.2 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 transmitting of confidential information;
- guarding against inappropriate and excessive personal use.

13. NON-COMPLIANCE

13.1 Any breach of this policy can result in disciplinary action up which may result in dismissal.

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

14. LIABILITY

14.1 The HSC does not accept any liability that may arise from employees using business email for personal use e.g. personal use of the email in response to spam, which may at a later stage result in fraud.

14.2 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.