NIPEC/16/14

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Information Technology Ethical Code and Computer Usage Policy

July 2016

Review date: June 2019

Centre House
79 Chichester Street
BELFAST
BT1 4JE

Tel: 0300 300 0066

www.nipec.hscni.net

Contents

1 Introduction

NIPEC users (staff and council members), hardware, software, telecommunications, facilities and data together form an IT system that is highly effective and productive. However, all IT systems involve certain risks that must be addressed adequately through proper controls. The policies contained in this document represent the organisation's commitment to assuring confidentiality, integrity, availability and control of NIPEC's IT resources.

Within NIPEC, it is essential for each user on the network to recognise their responsibility in having access to vast services, sites, systems and people. The user is ultimately responsible for their actions in accessing network services.

The "Internet" or "The Net" is not a single network; rather, it is a group of thousands of individual networks that have chosen to allow traffic to pass among them. The traffic sent out to the Internet may actually traverse several different networks before it reaches its destination. Therefore, users involved in this internet working must be aware of the load placed on other participating networks.

Within the Internet or other areas, users may find themselves within other networks (and/or the computer systems attached to those networks). Each network or system has its own set of policies and procedures. Actions, which are routinely allowed on one network/system may be controlled, or even forbidden, on other networks. It is the user's responsibility to abide by the policies and procedures of these other networks/systems. Remember, the fact that a user **can** perform a particular action does not imply that they **should** take that action. The use of the network is a privilege, not a right, which may temporarily be revoked at any time for abusive conduct.

The contents of this document are applicable to all IT resources at all levels within the organisation, whether maintained in-house or managed externally and are mandatory on all users, and others having access to and/or using the IT resources of NIPEC. The contents applies to all automated technologies currently in existence and to any new automated technology acquired after the effective date of this policy document.

1.1 NIPEC

1.1.1 The Environment

NIPEC's IT system, is managed through a Service Level Agreement (SLA) with the Business Services Organisation, Information Technology Services (ITS) and operates on a Cat 5 RJ45 cable environment, which links each desktop machine to the main NIPEC information server (accessible via the N Drive), that is located in BSO, ITS, Centre House. Within the organisation, there is a common PC Platform using a common operating system of Window 7 Enterprise.

Each machine links to the NIPEC Server (N Drive), via network points located within each office. These points are managed by two Cisco C3kx NM10 Switches, which are located within the NIPEC Computer Storage Room.

Whilst using the network, users may make use of a number of shared resources, e.g. the Xerox Multi-Devices, as well as files and folders (provided the user has the appropriate security permission).

The NIPEC Server is explained in more detail below: -

NIPEC Server
This server contains all the Email mailboxes (accounts and messages), allows Internet access from each desktop within the organisation, the Internal Filing Structure (which mirrors the structure of Central registry) as well as holding some software (for installation on demand). Each member of staff has a small area (folder) on the server to store items that is backed-up on a nightly basis. Access to these folders is restricted to the specific user, and the ITS (for maintenance purposes only).

1.1.2 Equipment & Software

Each piece of IT equipment will be fitted with a security tag, which allows NIPEC to keep track of equipment purchased, in terms of both its IT Asset Register and its IT Location Register. The fitting of a security tag is also to deter potential thieves from removing equipment from Centre House.

For laptops, projectors and other portable equipment, users should take note of the following security best practice guidelines:

- Users should ensure that laptops, handheld devices, mobiles, etc are kept away from magnetic sources e.g. TV, Airport Human Metal Detectors. Magnetic fields can damage hard disks and mobile phone SIM Cards - this could result in data loss/corruption.
- Caution should be exercised especially at airports, where laptops are frequently stolen. Users are reminded not to place laptops and other equipment onto conveyor belts until the very last moment – always keeping an eye on it at all times as they walk through the metal detectors. **NEVER** carry equipment through the Airport Human Metal detector (Conveyor belt X-Ray machines are data safe).
- Laptops, Projectors and other equipment should not be left on view in an unattended car – If any user has a requirement to leave equipment in a car, it should always be placed in the boot.
- For the protection of NIPEC data, stored on laptops, each laptop has PGP encryption software installed, and the hard disk is encrypted. The encryption requires a password access prompt to be completed, before the laptop can be used.
- Whilst staying in a hotel, equipment (including data flash drives, although NIPEC has taken some steps to ensure that encryption is used to protect data where necessary) should never be left unattended in a hotel room. If necessary, equipment should be placed in the hotels safe.
- Staff should perform frequent backups of data stored on laptops and mobile phone directories.
- Mobile phones should be protected by the setting up of a PIN Code, which needs to be entered every time the phone is turned on.
- Protect laptop data by setting up access passwords to equipment – these should be changed regularly.

Copyright law protects all NIPEC Software. Any unauthorised copying is a violation of NIPEC Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software.

1.2 Computer Usage Guidelines

Due to the range of IT equipment that is used by users, both internally and externally, it is appropriate to outline a number of guidelines which should be adhered to in all circumstances. This will ensure that each user who accepts, as part of their role within NIPEC, a piece of IT equipment such as PC or a Printer, is committed to a standard IT directive that will ensure effective and secure use of such equipment.

- NIPEC users have valid and authorised user accounts and may only use those computer resources to which they are specifically authorised. Users may only use their account in accordance with its authorised purpose. Users are responsible for safeguarding their own computer account. Users should not let another person use their account unless authorised by the Head of Corporate Services for a specific purpose.

- A user may not change copy, delete, read or otherwise access files or software without permission of the Head of Corporate Services. A user may not bypass accounting or security mechanisms to get round data protection schemes. A user must not attempt to modify software except when intended to increase efficiency through user customisation and permission for that specific purpose has been given.

- A user may neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, engaging in non-productive or idle chatting, sending mass mailings or chain letters.

- Users should not intentionally interfere with the normal operation of the network, including the propagation of computer viruses, or sustained high volume of network traffic that substantially hinders others in their use of the network.

- Users should assume that any software they did not create is copyrighted. They may neither distribute copyrighted or proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.

- A user should disclose to the Head of Corporate Services misuses of computing resources or potential loopholes in computer systems security and co-operate with the HCS in their investigation of abuses. In connection with inquiries into possible abuses, NIPEC, with the assistance of ITS, reserves the right to examine files, programs, passwords, accounting information, printouts or other computing material without notice. Privacy of any electronic or printed material examined during an investigation of abuse that is not relevant to the investigation is guaranteed.

Any user who is found to be abusing or misusing any NIPEC Computing services may not only be responsible for a violation of this policy or user responsibility, but it may also violate the criminal code.

For members of staff ailure to comply with this code may result in action being taken under the disciplinary procedure.

Finally, NIPEC promotes the use of its computing facilities and seeks to improve the computer literacy of users. Reducing computer abuse provides more computing resources for users with legitimate computing needs. Every user is expected to adhere to this policy. A further detailed explanation of the types of Computer Abuse can be found in Appendix A.

1.3 Good Password Selection

1.3.1 Rationale

The object when choosing a password is to make it as difficult as possible for a “cracker” to make educated guesses about what you've chosen. This leaves him/her no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete. As a good guide, *HSC Password Policy* requires NIPEC users to include within their password at least one capital letter, with the overall length not being under 6 characters.

1.3.2 What Not to Use

- Don't use your login name in any form (as-is, reversed, capitalised, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your name of spouse or child.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or of the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

1.3.3 What to Use

- Do use a password with mixed-case alphabetic characters.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

An example method of Choosing Secure and Easy to Remember Passwords might be to choose a line or two from a song or poem, and use the first letter of each word. For example, “**J**ack **a**nd **J**ill **w**ent **u**p **t**he **h**ill **t**o **f**etch **a p**ail **o**f **w**ater' becomes “jajwuthtfapow**"**

1.4 Physical Security

All ICT equipment within NIPEC is tagged with a unique Asset Tag, and logged in the NIPEC Asset Location Register which is linked to the NIPEC Asset Register held by BSO, Finance. The Asset Location register is updated by the by the Corporate IT & Information Officer, when equipment is moved, purchased or disposed and BSO, Finance duly informed.

In addition to an Asset tag, all equipment is password protected, meaning in the event of a loss of device, data remains secured. All office laptops within NIPEC are connected to their physical space using a security cable for which the staff member has the release key. This release key should be stored in a secure location, and remains the responsibility of the designated staff member.

1.5 Use of Wi-Fi within NIPEC

NIPEC, through BSO ITS, are part of a Wireless Configuration available to HSC users with valid login and remote working credentials.

All those making use of the Wi-Fi connectivity within NIPEC, must adhere to the following:

- It is the user's responsibility to ensure the device used to access this service has an appropriate level of security and protection against malicious means. Anti-virus provision is the responsibility of the user.
- No software/hardware support will be given to those using the service.
- It is not acceptable to use the wireless connection for any (but not limited to) the following:
  - The creation, transmission, downloading or printing of any offensive, obscene, pornographic or indecent images, data or other material, or any data capable of being resolved into pornographic or indecent images or material;
  - the creation, display or transmission of material which is designed or likely to cause annoyance, inconvenience, unnecessary anxiety, threats or the promotion of violence;
  - the creation, display, downloading or transmission of defamatory or discriminatory material especially anything likely to promote religious or racial hatred;
  - the transmission or downloading of anything other than copyright free material;
  - deliberate unauthorised access (i.e. "hacking") to any facilities or services accessible on the network;
  - deliberate activities with any of the following characteristics: (i) attempting to introduce a computer virus; (ii) attempting to corrupt or destroy data; (iii) disrupting the work of other users.
- If you breach any of these terms and condition of use, your permission to use this service will be terminated.
- It is preferable for misuse to be prevented and NIPEC reserves the right to take appropriate measures to monitor your use of this service.

1.6 Remote Working

Access to Remote Working is available for both the Senior Management Team and council members within NIPEC and is subject to the HSC Checkpoint Remote Access User Guide and Policy.

Access is via the HSC Remote Access Gateway, from a NIPEC device using Checkpoint Endpoint Security VPN. This service is strictly for use with HSC corporate PCs/tablets.

1.7 Storage of Media and Data

All removable media (Encrypted USB Flash Drives, Removable Hard Drives, etc) that contain any NIPEC-related documents should be stored in a cool, safe place, preferably in a place which can then be locked at the end of the working day. Removable Media are

sensitive storage devices, which are affected by stray magnetism. For this reason, staff should never place them on top of their office machine or near speakers.

Flash Drives/Data Keys should always have the protective cover placed around the USB connector when not in use. Users should never leave disk in drives when not in use, especially during a reboot operation.

1.7.1 Personal Information

Individual information includes academic, research, personal and all other records created and managed by individual staff members. As authors of such information, individuals are therefore responsible for securing and protecting their information.

Individual information should be protected based on the level of risk associated with its loss or misuse and individual staff have a responsibility for securing their own information and should take action to assure their individual data is protected to the level they deem adequate.

1.8 Disposal of Equipment/Media

Equipment which has come to the end of its usability within NIPEC is subject to an assessment by the HSC with the assistance of ITS, based on age of device, speed, connectivity, etc.

Since the policy default is that all IT equipment which stores or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.

Any equipment disposed of will be assessed by the HSC in collaboration with ITS and will be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2006.

2 Email & Internet

2.1 Rationale

The increased use of electronic mail (i.e., e-mail) and other Internet technologies provided to NIPEC users, such as the World Wide Web (WWW or "the Web"), provides NIPEC staff with access to a large professional and public audience. E-mail, the Internet and other network technologies have become fundamental tools within NIPEC, especially in the areas of research, administration and education, as well as popular mechanisms for global information distribution and access.

All NIPEC users are reminded that NIPEC e-mail and Internet services are offered under the understanding that the user accepts that they *have a duty to protect and conserve NIPEC property and shall not use such property, or allow its use, for other than authorised purposes."*

Examples of prohibited uses include:

- Unlawful or other malicious activities prohibited on NIPEC property.

- Display and/or printing of material or images that are sexually explicit, discriminatory or intended for harassment purposes.
- Forging email headers to disguise the true sender of the message, and any other activities that violate Local, UK, or European Law.
- Abusive language in either public or private messages.
- Computer games (unless used as a training tool).
- Misrepresentation of oneself or NIPEC.
- Activities that could cause congestion and disruption of networks and systems, such as the sending or forwarding of chain letters, violation of copyright, license agreements or other contracts. Example, copying and using signature for business purposes from a site where there is a clear limitation for personal use only;
- Downloading any information which could be considered illegal or offensive, e.g. pornographic, racist or sectarian material;
- Successful or unsuccessful attempts to gain unauthorised access to information resources, i.e., 'hacking';
- Using or knowingly allowing someone else to use any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services or other things of value by false pretences, promises or representations;
- Without authorisation destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the availability and/or integrity of computer based information and/or information resources;
- Using the Internet/Intranet for political lobbying;
- Violation of Copyright.

The use of Email and Internet technologies is encouraged within NIPEC, as the availability of search and retrieval tools on the Web provide the organisation with increased opportunities to use these technologies for gathering and disseminating information in their decision-making processes. Email & Internet technologies may be a mechanism for staff training and development of skills, and since BSO IT Services are supporting the entire Health network, there usually is no cost for individual use of e-mail and the Internet.

However, users are reminded that personal use of the technology should only be made at appropriate times (e.g., breaks, lunch time, before or after work). Any misuse of these Internet facilities by a member of staff will be brought to the attention of the HCS.

Line mangers should ensure that new employees and any other authorised users of NIPEC's Network are informed of appropriate uses of NIPEC resources as part of their introductory training or orientation.

2.2 Email

All NIPEC staff has access to IT equipment, and in order to take full advantage of such equipment, email should be the preferred means of communication within NIPEC. Within NIPEC hard copies of correspondence should not be forwarded between staff when email could complete the task more efficiently and cleanly.

The email facility should be used for all internal messages within NIPEC, including the booking of conference rooms/meetings between staff, requests for information, and where possible, correspondence with all external contacts. NIPEC's email software, MS Outlook, should be used in partnership with other software such as MS Word, MS Excel, MS

PowerPoint, MS Schedule as well, in association with Blackberry handheld devices (where appropriate).

Whilst NIPEC would wish to see e-mail used as much regarding external correspondence it is recognised that this may not be possible in all cases. Hard copies of written correspondence may still be required by external organisations that either do not currently have the capacity to respond to e-mail correspondence or request a formal written response from NIPEC.

2.2.1 Email Content

Within email, the tone and content of a message is very important. Staff should carefully review messages before being sent. Remember, you are not face to face with the person to whom you are corresponding, and that they will not see a smile on your face indicating that you are joking or other body language indicating that the message does not mean exactly what it says. By the same token staff should not jump to conclusions about the "tone" of a message from another user.

Staff should never compose an email in upper AND lower case, as all upper case messages are often interpreted as SHOUTING at the recipient. For this reason, all email messages should be written in lower case.

The content of an email can be just as important as the tone, and all staff should bear in mind that some people receive lots of emails per day, and so a long email may be viewed as less favourable. Email messages should be concise and to the point. Staff should always be aware that the person to whom they are sending an email might not have a similar standard of equipment. For this reason, formatting within email is less important, as many e-mail software cannot handle messages in fancy fonts, and colours, resulting in messages coming in as utter gibberish or in the worst case, crash your e-mail software.

With regard to salutations, staff need to evaluate each situation. If a person is normally addressed as Miss/Mrs/Ms/Mr. Smith then there is no need to alter this in relation to email. If the person is usually called by their first name then something along the lines of "Dear Tom" or just "Tom" would be appropriate. If staff are unsure, they should stick to the formal salutation - It's the safest bet.

Within the content of any email message, staff should refrain from using what are called *Flames.* A "flame" is an inflammatory or critical message that might trigger an angry response.

2.2.2 Attachments and Replying

Using NIPEC's email software, it is possible to forward/send e.g. MS Word documents to NIPEC colleagues, or even to external contacts. However, users should be aware that external contacts may not have similar equipment as contained within NIPEC, and as a result may cause problems at the recipient's site.

Attachments should only be sent when it is beneficial to both parties, e.g. in the case of a group working on a report. However, attachments can cause problems within the system, as they require quite a large amount of memory, to enable such messages to be delivered. Users are reminded that all email, either internal or external, has an effect on the external

network managed by BSO IT Services, and in fact external attachments over 10 Mb have the capability to cause serious problems for the HSC network as a whole.

With this in mind, **users should limit the size of attachments to 6-7 Mb**.

Users should also be ware of the danger of *threads*. Threads are generated by a series of responses to an original message. Where there are several parties to a discussion, and instead of starting an entirely new message to reply, users continue with the thread by pressing the "reply" button.

An Example of Threading
Keeping the thread information together makes it easier for all participants to follow the discussion; however it does cause message subjects to get very long.

2.2.3 Use of Encryption

Encrypting an email message protects the privacy of the message by converting it from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Any recipient without the corresponding private key sees garbled text.

This requires both sender and recipient to share their digital ID.

The process is below

Encrypt a single message
1. In message that you are composing, on the **Options** tab, in the **More Options** group, click **Message Options** Dialog Box Launcher .
2. Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box.
3. Compose your message, and then click **Send**.

2.2.4 International use of Email

Due to the huge reduction in telephone costs, over 120 countries use email to communicate internationally. One of the major advantages of email in an international sense is that it cuts across the world's cultures and spans all time zones, however, it is necessary to keep the following cultural nuances in mind when sending email abroad.

1. **Patience** At times email may be sent that will arrive during a recipient's off-work hours, or on a holiday that the author may not be aware of, and as a result a response may not be written for a few days. Users should be patient before re-transmitting the same message or sending a follow up message.

2. **Time and Dates** When sending an international email that includes dates and times, staff should ensure to translate using date and time conventions for the appropriate country. Remember that the Americans always put the month first so 1/4/97 is not April fool's day but the 4th of January.

Delivery of email within Centre House is completed within a matter of a few seconds, however delivery to national and international destinations may take a little longer, sometimes a few of minutes, to a few hours. Any longer and there is probably some kind of

problem. This delay is mainly due to the number of mail systems that your message must go through on its way to a destination. No matter how far away the recipient is, email is guaranteed to beat that of the normal postage service, or “snail mail”, as it is also termed.

2.2.5 Personal use of Email

Emails which are sent from NIPEC staff will contain the following disclaimer:

Disclaimer
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 HSCNI. 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 HSCNI takes precautions in scanning outgoing emails for computer viruses, no responsibility will be accepted by HSCNI in the event that the email is infected by a computer virus. Recipients are therefore encouraged to take their own precautions in relation to virus scanning. All emails held by HSCNI may be subject to public disclosure under the Freedom of Information Act 2000.”

It should also be noted that all emails to an external source, should contain the strapline regarding NIPEC’s online portfolio, and include the sender’s name, and contact details, such as set out below

Name
Title
NIPEC

Northern Ireland Practice and Education Council for Nursing and Midwifery,
Centre House, 79 Chichester Street, BELFAST, BT1 4JE
Direct Line e.g. 028 9536 xxxx
Mobile Number e.g. xxx xxxx xxxx
http://www.nipec.hscni.net

NIPEC

INVESTORS IN PEOPLE

https://nipecportfolio.hscni.net
Visit NIPEC’s new online portfolio which replaces the Development Framework website. Register to create your own electronic portfolio and access the competence assessment tools and the learning activities resources. It's easy to do, free to access and it is a secure site.

With the exception of unplanned leave and the need for NIPEC to put in place alternative arrangements to enable the work of the organisation to continue when a member of staff is absent from work, all personal email should remain private between the author and the recipient. Anyone found to be attempting to gain unauthorised access to another staff member’s mailbox will face disciplinary action under NIPEC’s disciplinary policy. However, as email is a very insecure form of communication, staff should be reminded that they should not be sending emails that they do not wish other members of staff to see. Under no circumstances should attachments of a confidential nature be sent via email, especially to external recipients.

Personal (or any other type of) email messages should not deliberately contain viruses, either in the main body or in attachments. Staff should ensure authenticity of authors and recipients, before opening any form of email communication. In-house HSC Anti-Virus protection should not be relied upon, to prevent damage to current NIPEC systems. The Corporate IT & Information Officer can advise on the procedure of dealing with emails from unknown sources or dubious sources. This should be sought before any such message or attachment is opened.

2.2.6 Best Practice Methods for Email

The following guidelines are intended to enable users to make use of the email system in a safer way.

1. Do not open attachments from unknown senders.
2. Be suspicious of email with attachments even if you do know the sender.
3. Don't open attachment unless absolutely certain of its content.
4. Beware odd Subject lines.
5. Be cautious of files downloaded from HTML formatted email, as this format often contains viruses that are difficult to detect.
6. Junk email and chain letters are **forbidden**, and should not be opened as they often contain viruses.
7. The identity of an email sender can be faked, so if you receive an apparently legitimate email requesting sensitive information, make sure to get verbal confirmation of the request before fulfilling the request.
8. Be sure that all sensitive internal documents, are always marked "**For internal use Only**"

2.2.7 Procedures

Given the move towards becoming PaperLite, i.e. that electronic files are stored primarily on the NIPEC Server, with a view of eliminating unnecessary amounts of paper within NIPEC, it is important to state some procedures on how the use of email relates to this issue.

SENDING EMAILS

- DO NOT send email messages in addition to a postal letter. All communication (where possible) should be carried out electronically.
- Save only relevant messages in an appropriately named folder, for easy retrieval. Saving every message that you have sent, is a drain on the Server storage, and therefore restricts the normal operation of the Server.
- DO NOT use the urgent flag too much, as other will learn to treat your email at the same priority as other email.
- DO NOT use the Delivery and Read receipt tags indiscriminately, as they create a large number of additional emails that the Server must deliver. Such receipts should only be used to confirm that an important action has been carried out.

STORING

In order to minimise the storage of e-mails under the ITS, SLA e-mails are archived after 3 months to an archive folder.

DEALING WITH SPAM

What is Spam?

SPAM is defined as an unsolicited electronic mail sent to one or many users. Due to the nature that Internet Mail works, it is very easy for "spammers" to send thousands of mail messages while incurring little cost to themselves. The main problem is that this form of advertising costs everyone else on the Internet. Internet Service Providers, such as Freeserve and BT, must relay messages and users must pay in the form of subscription and telephone charges to download SPAM. That's not to mention the time taken to sort SPAM mails from everything else. Typical SPAM mails include Chain letters, "Get Rich Quick" or "Make Money Fast" (MMF) schemes, Offers of phone sex lines and ads for pornographic web sites and Quack health products and remedies.

Typical emails are delivered in the following manner: -

rb484881554@sei.de	May 4 2006	BOOST YOUR SEX APPEAL AND CHANGE YOUR SOCIAL ...
profits900@aol.com	May 4 2006	Hot New Casino No Downloads
rb484873597@sfx.de	May 4 2006	Hi Sexy (343897)
cannonman5@hotmail.c...	May 4 2006	GET THE MOST OUT OF YOUR MARKETING DOLLAR!
cannonbro28@hotmail....	May 4 2006	REEL FUN CHARTERS!!!
cannonbro28@hotmail....	May 4 2006	Viagra OnLine - Instant Service - Overnight D...

Often SPAM is sent through 'trial' Internet accounts making it hard to trace, or return addresses are disguised. Sometimes hitting 'reply' merely confirms to the spammer that your address is active further encouraging these activities.

- NEVER reply to SPAM, as this will only confirm to the spammer that your email address is valid.
- If a user registers for something online, then they should ensure that they untick the box that allows them to be kept informed of changes. Many internet companies offer their list of subscribes to other "selected" parties and this could lead to increased awareness of NIPEC email addresses resulting in increasing junk emails.
- When subscribing to a Newsletter, users are advised to keep their subscription confirmation email in a separate folder for reference. Using this method will remind staff how to cancel subscriptions at any future date.
- If a user makes use of notice boards, or newsgroups, then the user is advised to ask the IT & Information for an additional email address, so as to prevent spammers getting main NIPEC addresses.

2.3 Internet

The Internet and the internal Health Service Intranet is accessed via NIPEC's network from each user's computer. All connections to the Internet/Intranet should be made through NIPEC's network, and as a result through the main HPSS network managed by BSO IT Services.

By being part of the HSC IT network each NIPEC machine is constantly checked for viruses, either resulting from any internal work or any information received from an external source. Under the SLA, with ITS, external users can only be allocated access to the NIPEC network after an 'Infra' has been raised to request permission.

Any staff member who has been allocated a laptop, or any other portable device, to enhance their work within NIPEC, should ensure that machines are not exposed to other networks or software which may not be as secure as NIPEC's environment.

2.3.1 Internet Content

Along similar lines of email use, staff are permitted and encouraged to make use of the Internet/Intranet facility offered by NIPEC, providing its use does not have an effect on that staff member's role or function within NIPEC.

Users are reminded that the sites that are visited by users are monitored and controlled by BSO, ITS security procedures and users must adhere to the prohibited use policy.

Any users who is involved in the downloading or transmission of any type of pornographic, sexually suggestive pictures or written materials will be investigated under NIPEC's disciplinary policy, which could lead to revocation of access privileges, and may face criminal charges and termination of contract.

2.3.2 Internet Publishing

The Corporate IT & Information Officer is responsible for the overall maintenance of the NIPEC website and no new material, with the exception of up-dating material, should be placed onto the web page without the knowledge of the above and the authority of the IT Governance Group.

The IT & Governance Group has overall responsibility for the governance of the NIPEC website and microsites to ensure that the content is up to date, and prevent irrelevant information being placed online. In addition to this, staff should be aware that the Copyright Law is in operation online, as well as in written form. Therefore all material placed online by NIPEC staff is assumed to adhere to the copyright law and legislation.

2.3.3 Internet Groups/Newsgroups

Users may make use of Newsgroups for business purposes. A Newsgroup is a kind of electronic notice board, which can be set up on any subject, and any number of people may "post" things to that notice board. The notice board is available to anyone and can be very useful, especially for issues for fields, which are constantly changing e.g. medicine, and gives user's access to the thoughts of leading experts in particular fields. A Newsgroup is commonly known as a "One-to-Many Communication", as a user is able to correspond to many people via one message. As with any email message, the standard rules outlined in section 2.2 should apply.

Users should be aware that many emails are involved within Newsgroups and it is possible to receive 60-80 emails per day on a subject, and that individuals speak for themselves, and what they say does not necessarily represent their organisation (unless stated explicitly).

The use of Newsgroups has a detrimental effect on resources, simply due to the volume of email messages that membership creates. It is for this reason that staff are advised to think carefully about membership of Newsgroups and that there should be a solid beneficial reason for membership of any such list.

Participation of any newsgroup with a Political or Sexual nature is strictly forbidden.

2.3.4 Downloading of Internet Files

The downloading of any file can be hazardous, mainly due to the uncertainty of the location to which users are directed to download from. Users should therefore ensure, as far as possible, that the site can be identified as the certified source of the file being downloaded.

Users should at all times work within any conditions which may be placed upon external users of Internet sites, as breach may be viewed as “hacking”. To protect a site’s copyright laws, users are only permitted to download files, when/where the Internet site allows such activity and where such downloads are not in violation of its copyright.

Users are reminded that the downloading of files may result in the capturing of viruses or even changes within machine configurations, which could result in the machine being inoperable. For these reasons, users are asked to exercise extreme caution when downloading, and the Corporate IT & Information Officer should be consulted if a user is in any doubt.

2.3.5 E-Commerce

Users are forbidden to use NIPEC equipment and services to order any form of personal goods or services. **The use of the Internet/Email is for business purposes and not for situations where staff can enter into a personal agreement with an external supplier, which could result in NIPEC being liable for any costs of such goods**.

In exceptional circumstances, staff may use the Internet to make business purchases on behalf of NIPEC, as long as the restrictions of Internet Use are not breached.

APPENDIX A - COMMON FORMS OF COMPUTER ABUSE

Computing resources are valuable, and their abuse can have a far reaching negative impact. Computer abuse affects everyone who uses computing facilities. The same morality and ethical behaviour that applies in the non-computing environment applies in the computing environment.

In providing computing resources, NIPEC has the responsibility of informing its users of the rules, regulations and procedures regarding their usage. Computer users are responsible for understanding these rules so that they can abide by them. The following topics are areas of abuse:

PRIVACY

Investigating or reading another user's files without prior agreement, is considered the same as reading papers on someone's desk - a violation of their privacy. Reading unprotected files is rude; reading protected files, by whatever mechanism, is considered the same as "breaking and entering".

Violations include:

- Attempting to access another user's computer files without permission
- Supplying or attempting to supply false or misleading information or identification in order to access another user's account;
- Deliberate, unauthorized attempts to access or use NIPEC's computer facilities, networks, systems, programs or data;
- The unauthorized manipulation of NIPEC's computer systems, programs or data.

THEFT

Theft includes the stealing of any property belonging to NIPEC, or any other person or organisation that uses facilities at NIPEC. Unauthorised use of Internet is also considered to be theft.

Violations include:

- Using subterfuge to avoid being charged for the use of computer resources;
- Abusing specific computer resources, removing any computer equipment (hardware, software, data, etc.) without authorisation from the Corporate IT & Information Officer, or NIPEC's Management; copying, or attempting to copy, data or software without proper authorisation.

VANDALISM

Any user's account, as well as the operating system itself, is a possible target for vandalism. Attempted or detected alteration of user system software, data or other files, as well as equipment or resources disruption or destruction, is considered vandalism.

HARASSMENT

Harassment of other users may be the sending of unwanted messages or files. *Violations* include:

- Interfering with the legitimate work of another user;
- The sending of abusive or obscene messages via computers;

- The use of computer resources to engage in abuse of computer personnel or other users.

MISCELLANEOUS

Other uses commonly considered unethical, such as:
- Unauthorised and time-consuming recreational game playing.
- Using computer accounts for work not authorised for that account.
- Sending chain letters or unauthorised mass mailings.
- Using the computer for personal profit or other illegal purposes.
- Personal advertisements.