NHS
North Yorkshire and York

Title:	E-mail and Internet Policy
Reference No:	
Owner:	Angela Wood, AD of IM&T
Author:	Shaun Macey, IT Manager
First Issued On:	
Latest Issue Date:	
Operational Date:	1st August 2009
Review Date:	1 year
Consultation Process:	IM&T Steering Group,
Policy Sponsor:	Bill Redlin, Director of Performance
Ratified and Approved by:	JNCC, LNC, Governance Committee
Distribution:	All staff in line with the PCT Policy on Policies
Compliance:	Mandatory for all permanent & temporary employees, contractors & sub-contractors of North Yorkshire and York PCT
Equality & Diversity Statement:	This policy has been subject to a full Equality Impact Assessment

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERSION No
dd.mm.yy	Name & title	E.g. 'New Policy' or where amendments only to an existing policy - state section(s) where amendments made	
03.12.08	Shaun Macey, IT Manager	General amendments and additions to draft document.	0.06
10.12.08	Shaun Macey, IT Manager	General corrections – final draft version for Directors.	0.07
15.12.08	Shaun Macey, IT Manager	Comments after Directors meeting	0.08

08.01.09	Shaun Macey, IT Manager	Changed North Yorkshire & York PCT to 'NHS North Yorkshire & York'	0.09
26.02.09	Shaun Macey, IT Manager	Addition to 'personal use' section	0.10
22/7/09	Angela Wood	Amended 2.3.2 – Personal use	Final
25/8/09	Jane Grayson IG Manager	Amended 'Personal Use' section and added – 'Personal Blogs and websites'	Revised
17/9/2010	Oliver Tipper, Communications Manager	Amended section 2.4 to include more guidance on the use of social networking sites and posting personal content	Revised

Contents

PREFACE

This Policy is made between NHS North Yorkshire and York and the recognised staff side organisations, using the mechanism of the JNCC. It will remain in force until superseded by a replacement Policy, or until terminated by either management or staff side, giving no less than six months notice. The purpose of the notice to terminate the Policy is to provide the opportunity to both parties to renegotiate a replacement Policy. Withdrawal by one party, giving no less than six months notice, will not of itself invalidate the agreement. If agreement cannot be reached on a revised policy, then either party may refer the matter to the Advisory, Conciliation and Arbitration Service (ACAS) for conciliation.

1 INTRODUCTION

1.1 Rationale

1.1.1 In common with other NHS organisations, the PCT operates both internally and externally accessible e-mail facilities and provides access to the Internet through its connection to the NHS wide area network, N3. The N3 network provides access to both NHS-specific websites (prefixed nww.) and the world-wide web (prefixed www.). Access to the N3 network is provided to the PCT under the terms and conditions of the Connecting for Health Information Governance Statement of Compliance (IGSoC).

1.1.2 This policy sets rules and provides guidance on the use of the PCT's e-mail and Internet facilities.

1.2 Scope

1.2.1 The policy applies to:

a) All full-time and part-time employees of the PCT, and to contracted third parties (including agency staff), locums, students and trainees, secondees and other staff on temporary placements with the PCT, and staff of partner organisations with approved access.

b) Other individuals and agencies who may gain access to data, such as volunteers, visiting professionals or researchers, and companies providing IT services to the PCT.

c) GP Practices are strongly advised to adopt this policy as best practice.

1.3 Principles

1.3.1 E-mail and the Internet are fast and effective electronic means of communicating and gathering information that can enhance the efficiency and effectiveness of staff across the PCT.

1.3.2 The facilities exist primarily for the purpose of conducting PCT business but can also be used for permitted personal purposes on a limited basis.

1.3.3 E-mail carries the same legal status as other written documents and should be used with the same care.

1.3.4 E-mail allows electronic records of communications over a period of time to be maintained and systematically managed and referenced.

1.3.5 The Internet provides a wide-ranging source of information and knowledge but offers no guarantee of accuracy, reliability and authenticity.

1.3.6 The Internet and N3 are now the primary means of communicating policy by the Department of Health within the NHS.

1.3.7 The PCT will use these facilities to the full (but within the constraints of available resources and technology) in communicating and cascading information throughout the organisation.

1.3.8 E-mail and Internet facilities employ complex technology that can **not** be guaranteed 100% reliable, and staff should not rely wholly and solely on them for critical business processes.

2 INTERNET AND E-MAIL ACCEPTABLE USE POLICY

2.1 Core Principles

2.1.1 Staff will have access to e-mail and the Internet in accordance with national targets.

2.1.2 Recognised staff organisations, including Trade Unions, will have access to e-mail and the Internet.

2.1.3 Personal use of the facilities will be limited and within prescribed areas.

2.1.4 Safeguards will be established to protect the security, integrity and availability of the PCT's IT systems.

2.1.5 The requirements of relevant Acts of Parliament and mandatory national policies will be observed at all times.

2.1.6 Guidance on e-mail etiquette will be observed in accordance with Section 2.2.14 of this document.

2.1.7 Guidance on housekeeping to ensure efficiency in the operation of the PCT network and personal folders will be observed.

2.1.8 The policy relates to staff using the Internet and e-mail over the PCT network either directly or remotely (via strong authentication token).

2.1.9 The use of the Internet and e-mail is routinely logged by the PCT's Informatics Department for security and auditing purposes, and if required, usage can be monitored on an individual basis.

2.2 Common Standards – E-mail

2.2.1 **Access** – E-mail is available to all staff who are registered as users of the computer network. All users are required to complete an 'E-mail & Internet Services - User Code Of Connection' form which needs to be submitted to the PCT's IT Service Desk before access is granted. A copy of this form can be found in *Appendix A*. This form must be signed by the individual.

2.2.2 **Personal Use** – Although frequent personal use of e-mail facilities is discouraged, *limited* personal use will be permitted provided that the content of the message is appropriate, i.e. is not likely to cause offence. Employees should regard this facility as a privilege that should normally be exercised in their own time without detriment to the responsibilities of their job and not abused. Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. Staff should be aware that both private and business use of e-mail is routinely logged by the PCT's Informatics Department for security and auditing purposes, and if required, usage can be monitored on an individual basis. Any Personal emails should include the word 'Personal' in the title of the email.

2.2.2.1 Staff should not use the e-mail system to conduct personal transactions in pursuit of their own commercial or business interests, nor in such a way as to implicate the PCT in those transactions.

2.2.3 **Confidentiality** – Confidentiality can be compromised, especially when using Internet-based e-mail systems. Employees must not send sensitive information (**this includes personal, patient-identifiable, financial, HR and commercially sensitive information**) via the Internet, other than through an approved application – currently between NHSmail accounts – i.e. from one '@nhs.net' e-mail address to another '@nhs.net' e-mail address. It is good practice to anonymise the data. The principles of the Data Protection Act 1998 and the Caldicott guidelines must be adhered to at all times. These principles must also be adhered to when using any form of electronic discussion forum or Internet Messaging application.

2.2.4 In the interests of confidentiality, note that it is not acceptable to forward any PCT e-mail to any domestic e-mail account such as, but not limited to, Hotmail or AOL. If required, information from PCT e-mail systems should only be forwarded to an NHSmail account. To technically support this requirement access to domestic Internet based e-mail systems from the PCT network has been restricted

2.2.5 For additional guidance on information security, please see the PCT's Information Governance web page at: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm, and in particular the document titled 'Information minimum security measures'. Please contact the IT Service Desk if you have a requirement to send person-identifiable information via the Internet and are unsure how to do this securely.

2.2.6 **Disclaimers** – A disclaimer has been set up that will automatically attach to all out-going e-mail. This is designed to limit the PCT's potential liability with respect to information being communicated. Note – the disclaimer is not meant to preclude the user from undertaking fundamental checks before sending the e-mail, e.g. checking the content for accuracy, correct addressee, etc.

The content of the PCT disclaimer is as follows:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

This e-mail may contain confidential and privileged information. If you are not the intended recipient please accept our apologies; please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful. Please inform us that this message has gone astray before fully deleting it.

The Primary Care Trust has legal obligations under the Freedom of Information (FOI) Act to disclose records unless a legal exemption applies (including contract and tender information). Our staff, therefore, are not authorised to receive information that is provided 'in confidence'.

Computer viruses can be transmitted via e-mail. The recipient should check this e-mail and any attachments for the presence of viruses. The Primary Care Trust accepts no liability for any damage caused by any virus transmitted by this e-mail.

Communications systems may be monitored and/or recorded to secure the effective operation of the system and for other lawful purposes.

NHS North Yorkshire and York

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Please note this has been set up automatically by the IM&T Department and should not be set up as part of your individual auto-signature.

2.2.7 **Housekeeping** – The amount of e-mail stored in an individual's Inbox should be kept to a minimum. Both received and sent e-mails should be reviewed on a monthly basis and deleted when no longer required. E-mails that need to be saved should be moved to a personal folder. Note that if we receive a Freedom of Information request, an individual may be obliged to search through all messages in their mailbox – effective housekeeping will make this process more straightforward.

2.2.8 When an e-mail is deleted it stays in the Deleted Items folder and needs to be deleted again from this folder to permanently remove it.

The PCT reserves the right to store historical e-mail messages on its archive servers in order to reduce storage requirements and maintain performance on its main e-mail systems. This process will be transparent to staff as archived e-mail headers will still appear in an individual's mailbox, with messages being automatically retrieved from archive by users on an as needed basis.

Care should be taken when sending file attachments as these are typically large and may cause network congestion. File attachments should only be sent when absolutely necessary and should be deleted or

saved to a network drive by both sender and recipients as soon as is practicable.

Any file attachments for general circulation (e.g. Staff Bulletins) should **not** be circulated to staff via e-mail using distribution lists. Instead, these should be made available via the PCT's Intranet site, and links to the documents should be circulated via e-mail.

Please contact the IT Service Desk if you need assistance or advice regarding any aspect of e-mail housekeeping.

2.2.9 **Harassment** – It is strictly forbidden to send messages that contain offensive or harassing statements or language, particularly with respect to race, national origin, gender, sexual orientation, age, disability, religious or political beliefs. Remarks sent by e-mail that are capable of amounting to harassment may lead to complaints of discrimination under the Sex or Disability Discrimination Acts, or the Race Relations Act. A breach may result in disciplinary action and/or removal of facilities.

2.2.10 **Defamation** – The ease of use of e-mail can lead to unguarded and impetuous comments being made, which in turn could be classified as defamatory. Employees are therefore advised to take care when drafting e-mails to ensure that the content is not libellous. These principles should also be adhered to when using any form of electronic discussion forum or Internet Messaging application. A breach may result in disciplinary action and/or removal of facilities.

2.2.11 **Copyright** – Under the Copyright, Designs and Patents Act 1988, copyright law can be infringed by making an electronic copy or making a 'transient' copy (which occurs when sending an e-mail). Copyright infringement is becoming more commonplace as more and more people forward text, graphics, audio and video clips by e-mail. Employees must not, therefore, copy, forward, or otherwise disseminate third-party material without appropriate consent.

2.2.12 **Viruses** – Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the PCT. If any viruses are found or suspected, the user should stop using the PC, disconnect the network cable, and the IT Service Desk must be informed immediately.

On no account should individuals send or forward virus warnings to other users unless instructed to do so by the IT Service Desk.

The downloading and subsequent use of any software received via e-mail, without the prior approval of the IT Security Officer, is strictly forbidden. This includes screen savers.

2.2.13 **E-mail Security –** As an extra security measure, any e-mails addressed to PCT staff will be stopped by anti-virus software and held in quarantine if an e-mail is suspected of:

- Containing a virus
- Containing a password protected or encrypted attachment
- Containing a corrupt attachment

If your e-mail is held in quarantine you will receive an automatic e-mail informing you of this.

Quarantined e-mails are held in a separate mailbox that is accessed by the IT Service Desk twice daily. They check the status of each e-mail and either release them to the user or delete them, depending on the issue.

2.2.14 **Etiquette** – The following should be observed:

- E-Mails should always be signed off with the name, job title and contact details of the sender. This can be effectively set up as an auto signature. If you need assistance with setting this up please contact the IT Service Desk.
- Don't make the signature too long, too large, or add animation or graphics as this will take up unnecessary disk space.
- When away from the office staff should, wherever possible, use the 'Out of Office' feature to inform colleagues of their time of return, and provide an alternative contact if appropriate.
- There are security implications around messages having a blank subject, therefore always complete the subject field to indicate the contents when sending an e-mail. It will assist the recipient in prioritising the opening of e-mails and aid future retrieval of messages.
- Always use mixed uppercase and lowercase letters to improve readability.
- Care should be taken with content. Nothing should be written in an e-mail that would not be written in a letter or said to someone face to face.

2.2.15 **Formation of Contracts** – E-mail is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of employees inadvertently forming contracts on behalf of the PCT or varying contractual terms to which the PCT then becomes bound. Employees should take due care when drafting the words of an e-mail so that they cannot be construed as forming or varying a contract when this is not the intention.

2.3 Common standards – Internet

2.3.1 **Access** - All users are required to complete an 'E-mail & Internet Services - User Code Of Connection' form that needs to be submitted to

the PCT's IT Service Desk before access is granted. A copy of this form can be found in *Appendix A*. This form must be signed by the individual.

2.3.2 **Personal Use** – Limited personal use of the PCT's Internet facilities is permitted, provided that the material accessed is appropriate and is not potentially offensive to others. The use of the Internet for personal transactions, such as booking reservations or tickets, or the purchase of any goods or services for personal use is permitted. Employees should regard this facility as a privilege that should not be abused and should normally be exercised in their own time and without detriment to the responsibilities of their job. Inappropriate or excessive use may result in disciplinary action and/or removal of this service.

- Two and a half hours weekly (approx. 30 mins. per day) is the maximum allotted time for access to leisure sites. For part-time staff this should be pro-rata.
- Leisure sites should only be accessed either before/after working hours, or during an allocated break.
- The PCT does not recommend use of credit/debit cards for payment over the Internet. If you choose to use them, only use credit cards on an https:// website address as these are more secure. The PCT can not be held liable for any losses or resultant fraudulent transactions following the use of an individual's credit/debit cards on the PCT network.
- Do not save any passwords or credit/debit card details to PC's or network drives as this information could be seen by other staff.
- Some "addictive" sites – e.g. eBay (auction site) have a quota set against them to allow only limited access.
- Staff should be aware that all Internet access is routinely logged for security and audit purposes, and usage can be traced to time, location and user name.
- Staff are accountable for any Internet sites accessed from their login, and should therefore logout or lock the PC each time they leave the room.

If any member of staff has a legitimate requirement for additional leisure access to the Internet, they should discuss with their Service Manager who should submit justification of this decision to the IT Service Desk. The request will then be considered at the next Informatics Programme Board meeting.

2.3.3 **Inappropriate Use** – Access to websites that contain inappropriate material is strictly forbidden, e.g. pornography, promotion of criminal or terrorist activities, promotion of cults, gambling, content or statements of a nature which are liable to cause offence to others, or any other material

likely to bring the PCT into disrepute. Please note this is not an exhaustive list.

- Access to inappropriate sites is blocked, but it is accepted that some sites may still be accessible. Employees should operate the 'Back' button immediately should they inadvertently access unsuitable material and contact the IT Service Desk so that further access to the site can be blocked.

- Downloading of inappropriate material shall be deemed a disciplinary offence and will be investigated under disciplinary procedures. However, the PCT notes that access to subjects and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances, e.g. sex education, youth advice, approved research, etc. If staff need access to such sites in order to do their job, then the appropriate Service Manager should approve the request and complete the form to request access to blocked sites (*Appendix B*) and return to the IT Service Desk for approval to the Informatics Programme Board.

- Staff should not use the Internet to conduct personal transactions in pursuit of their own commercial or business interests, nor in such a way as to implicate the PCT in those transactions.

- **Copyright** – Files must not be downloaded from the Internet and used in such a way as to violate copyright laws. Even if downloading is permissible under copyright law, there may be restrictions with regard to copying, forwarding, or otherwise distributing files and in addition may cause conflict with current systems. Software license agreements should be read and adhered to. Staff must not transmit copyright software from their computer via the Internet. Staff must not download or install any programs on PCT computers without prior consent from Informatics department.

2.3.4 **Viruses** - Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the PCT. All files downloaded from the Internet will be automatically virus checked before use. Employees must not independently load software onto their PC's (this includes screen-savers). All software installations must be arranged with the IT Service Desk.

2.3.5 **Internet Service Providers** – Internet access *must* be via the PCT's network in all instances. The use of modems on PCT sites is strictly prohibited and individuals must not independently arrange Internet access, via any means, direct with a commercial Internet Service Provider (ISP).

2.4 POSTING PERSONAL CONTENT TO THE WEB i.e. social networking, personal blogs, content-sharing websites etc.

2.4.1 This part of the policy and procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, including message boards and social networking or content-sharing sites etc) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

2.4.2 The PCT recognises that you may wish to publish personal content on the internet. For the avoidance of doubt, such activities are expressly prohibited during working hours and if using PCT IT systems, such activity must be conducted in agreed break periods.

2.4.3 If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of PCT staff and/or you discuss your work or anything related to PCT or its business, patients or staff, the PCT expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with PCT's policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for the PCT.

2.4.4 When someone clearly identifies their association with the PCT and/or discusses their work, they are expected to behave appropriately, and in ways that are consistent with the PCT's values and policies, their individual responsibility as a Trust employee, and with the relevant professional codes of conduct for NHS professionals.

2.4.5 You should be aware that information posted online is subject to precisely the same laws of defamation and libel as that which is published in hard copy. Therefore, you can be sued for libel for any defamatory statements you post about other individuals or organisations. You should be aware that this is a personal liability. The PCT would not and cannot offer any assistance whatsoever in dealing with any proceedings.

2.4.6 If you already have a personal blog, website or social network which indicates in any way that you work for the PCT you should report this to your line manager.

2.4.7 If you intend to create a personal blog, website or social network that will say that you work for the PCT, or in any way could identify you as someone who works for the PCT then you should report this to your line manager.

2.4.8 If a blog posting clearly identifies that you work for the PCT and you express any idea or opinion, you should be mindful of the points made above. It is also recommended that you add a disclaimer such as "these are my own personal views and not those of the PCT."

2.4.9 The following points relating to posting content on the internet will be treated as gross misconduct and would be dealt with under the PCT's disciplinary process (this list is not exhaustive):

- Revealing confidential information about the PCT in a personal online posting. This might include revealing information relating to the PCT's patients, clients, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.

- Criticising or embarrassing the PCT, its clients or its staff in a public forum (including any website). You should respect the reputation of the PCT and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise this with your line manager, use the PCT's grievance procedure or its whistle-blowing procedure.

2.4.10 If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your line manager.

2.4.11 If you are contacted by a journalist or someone from the media about your online publications that relate to the PCT you should seek advice from your line manager and the PCT Communications Team before responding.

2.4.12 Online publications which do not identify the author as a member of PCT staff, do not mention the PCT and are purely concerned with personal matters will normally fall outside the scope of this policy.

2.4.13 Staff who are heavily engaged in social networking, or are interested in using it as part of their work for the PCT, should contact the Communications Team on 01423 859616.

3 IMPLEMENTATION AND COMPLIANCE

3.1 Responsibilities of all Staff

3.1.1 All staff are obliged to adhere to this policy. It is the responsibility of the individual to ensure that they understand this policy. Managers at all levels are responsible for ensuring that the staff for whom they are responsible are aware of and adhere to this Policy. They are also responsible for ensuring that staff are updated with regard to any changes in this Policy.

3.1.2 Any breeches of this policy should be reported to the IT Security Officer

4 REFERENCE DOCUMENTS

- *Appendix A* contains the 'E-mail & Internet Services – User Code of Connection' form. This form must be signed and returned to the IT Service Desk before Internet and e-mail access can be provided.

- *Appendix B* contains the request form to unblock a 'blocked site'.

5 FURTHER INFORMATION

5.1.1 Further information can be sought from the IT Service Desk, e-mail itservicedesk@nyypct.nhs.uk or telephone 0844 822 1011.

6 CONSULTATION, APPROVAL AND RATIFICATION PROCESS

6.1.1 This policy and any updates will be submitted to the PCT's IM&T Steering Group (comprising key stakeholders from the local health community) for consultation and approval.

6.1.2 Thereafter, the policy will be approved and ratified through JNCC and LNC.

7 DISSEMINATION AND IMPLEMENTATION

7.1.1 This policy will be distributed to all directors, heads of service, senior managers and directorate managers for implementation within their areas.

7.1.2 Awareness of the policy will be raised through the PCT electronic staff newsletter and a copy of the updated version will be available via the PCT intranet.

8 DOCUMENT CONTROL INCLUDING ARCHIVING ARRANGEMENTS

8.1.1 This policy will be stored on the PCT's Intranet, on the policies and procedures section.

8.1.2 On review of this policy, archived copies of previous versions will be held by the Directorate Policy Coordinator on behalf of the Policy owner. The Directorate Policy Coordinator will keep an up to date list of the archived policies and their location. The Policy will be available as an archived document as soon as the latest version has been made available on the PCT Intranet/Internet.

8.1.3 To retrieve a former version of this policy, contact the Directorate Policy Coordinator.

9 REVIEW

9.1.1 This policy will be reviewed after one year and thereafter on an annual basis.

9.1.2 An extraordinary policy and procedure review will be initiated following any incident that arises which highlights the need to review this policy or following new legislation, Connecting For Health guidance, etc.

9.1.3 This policy will also be subject to review through internal and external audit mechanisms.

10 MONITORING

10.1.1 Monitoring of compliance with this policy through IT systems controls and management will be the responsibility of the PCT's Informatics Department.

11 EQUALITY & DIVERSITY

11.1.1 The PCT recognises the diversity of the local community and those in its employment. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. All strategies, policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

12 TRAINING AND AWARENESS

12.1.1 Policies and procedures will be made available on the PCT staff web site and will form part of the corporate and local induction of all staff. Awareness of new policies will be made via a cascade system from the designated staff member for policy management to all Service Managers for dissemination to staff as well as by the PCT electronic staff newsletter.

12.1.2 Any training requirements arising from this policy will be addressed by the Informatic Department's Training Team.

13 DATA PROTECTION ACT 1998 STATEMENT

13.1.1 The Data Protection Act 1998 protects personal data, which includes information about staff, patients and carers. Unlawful of unfair processing of personal data may result in the PCT being in breach of its Data Protection obligations.

14 DISCIPLINE

14.1.1 Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the PCT's disciplinary procedure.

APPENDIX A

NHS North Yorkshire & York
E-MAIL & INTERNET SERVICES – USER CODE OF CONNECTION

To be signed by all users of Internet and E-mail services.

Introduction

NHS North Yorkshire & York is able to provide Internet access to designated users via the N3 network because we have met the various security criteria required by Connecting for Health and BT (who manage the NHS's N3 network). This includes producing a PCT Security Policy, implementing physical and logical network security measures, provision of staff guidance documentation, and the Chief Executive signing a Statement of Compliance document agreeing to abide by the terms and conditions of that document or risk being disconnected from the N3 network

It is important that users of this service are aware of the security requirements, understand the implications of non-compliance, and agree to abide by the terms and conditions of this document.

Background

The Internet is an uncontrolled, unmanaged and largely unsupported world-wide network. It is a source of much valuable information, including subjects pertaining to the area of healthcare, however it is also an unrestricted source of much illegal and illicit material. Additionally, it has a large recreational attraction. Although it has been in use since the 1960's it has only recently been opened up to commercial use and consequently the pace of developments and usage far outstrips measures to resolve such issues as international law, policing, management and security.

Security

- Internet and e-mail services are available for work related purposes. Certain categories of "leisure" sites are available but should not be used to the detriment of your work in the PCT or the efficient running of the N3 network service.
- Websense software will ensure that sites containing illegal or offensive material are generally filtered into categories that are blocked and inaccessible. Sometimes sites slip through this safety net so staff are warned to be very careful, for example, with their use of Internet 'search' facilities.
- If legitimate access is needed to a specific site within a blocked category, please complete the form attached as *Appendix B* and send to the IT Service Desk.
- A default web site is accessed at sign on; this is the PCT Intranet site.
- Illegal or offensive material must not be accessed, downloaded or stored on any PCT computer.

- Illegal or offensive material must not be downloaded and sent as an e-mail attachment. This could be in breach of the Telecommunication Act and Obscene Publications Act as well as PCT policy.
- Copyright restrictions must be adhered to when downloading material.
- Unlicensed software must not be downloaded and installed on any PCT IT equipment.
- Any files downloaded legitimately must be virus checked before being e-mailed around the PCT.
- All Internet sessions are routinely logged for security and audit purposes - these logs are checked and retained.
- Where multiple users have access to a PC they must always use their own login and password.
- Any PCT IT equipment can be audited at any time by the Informatics Department, a representative of Connecting for Health, N3, or internal/external audit bodies.
- Internet browsing will significantly increase network traffic, so reducing the response of other critical network applications and services. It is in all users' interests to keep Internet browsing sessions to a minimum.
- Breaches of security, abuse of services and non-compliance with the PCT's Information Security policy or the User Code of Connection criteria may result in the withdrawal of e-mail and Internet services.
- A breach of the above could also result in disciplinary action being taken against a member of staff in accordance with the PCT's disciplinary procedure.

NHS North Yorkshire & York
Chief Executive

USER ACCEPTANCE
I have read and understand this document and agree to abide by the above security criteria.

User name (print) …… Date ……

Signature……

Division/Directorate……

or
☐ **I have not signed as I have further questions and would like to be contacted to discuss.**

(Please return a copy of this to NYY PCT IT Service Desk, Station Road Business Park, Station Road, Thirsk, Y07 1PZ)

APPENDIX B

INTERNET ACCESS TO BLOCKED SITES - APPLICATION FOR ACCESS

To be completed by Service Manager	
Address (URL) of the site(s) to be accessed	…… …… …… ……
Please allow access to the above site for (Name):	……..
Job title:	……..
Work base:	……..
Reason for access:	…… …… ……..
Is access permanent or temporary	Permanent / Temporary* *(*Delete as appropriate)* If temporary, please give dates as to when access should be removed.
Signed	…… (Service Manager)
Date	……

Please send the completed form NYY PCT IT Service Desk, Station Road Business Park, Station Road, Thirsk, Y07 1PZ) or e-mail itservicedsesk@nyypct.nhs.uk. Either the Service Manager's signature is required or the form should be e-mailed by the Service Manager.