NHS
North Yorkshire and York

Title:	**IM&T Acceptable Use Policy**
Reference No:	NHSNYY/004
Owner:	Director of Finance and Contracting
Author:	AD of Informatics
First Issued On:	February 2011
Latest Issue Date:	February 2012
Operational Date:	February 2012
Review Date:	February 2013
Consultation Process:	List stakeholder groups etc consulted
Policy Sponsor:	Director of Finance and Contracting
Ratified and Approved by:	Information Governance Steering Group
Distribution:	All staff
Compliance:	Mandatory for all permanent & temporary employees, contractors, sub-contractors of and those who work jointly with North Yorkshire and York PCT
Equality & Diversity Statement	This policy has been subject to a full equality & diversity impact assessment

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERSION No
Feb 2012	AD Informatics	Planned Review	0.001

NHS North Yorkshire & York

IM&T Acceptable Use Policy

February 2012

Review date February 2013

Contents

1 Scope

ADVICE:
IT equipment includes (but is not limited to) PCs, Mobile IT equipment and Printers.

"Other Organisations" could include NHS and outside agencies, e.g. local government.

This Acceptable Use Policy applies to all NHS North Yorkshire & York staff accessing the NYY network and the use of IT equipment and IT systems. GP Practices are strongly advised to adopt these guidelines as best practice.

All staff should be aware of their legal obligations and of the PCT's Information Governance (IG) and IT Security Policies and related procedures. See the following Intranet link for more information: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm

This document and any of the documents referred to are accessible on the PCT's Intranet site.

2 Information Security

2.1 Authorisation

ADVICE:
If a new member of staff will require computer access on their first day of work, line management should ensure that the username/password application is submitted **at least 5 working days in advance**.

Agency staff, temporary and non-PCT staff can be given a user account. Under no circumstances will generic or shared accounts be set up.

Contact the IT Service Desk for further details.

On request, the IT Service Desk will provide each member of staff with a personal username and password, which must be used for authentication to gain access to any PCT computer.

Usernames or passwords will only be issued when authorised by the appropriate Line Manager. A Computer Account Request form can be found on the PCT's Intranet.

When a password is issued the member of staff will be directed to a printed and/or electronic copy of this Acceptable Use Policy and will have the key points explained to them (Passwords, Confidentiality, Monitoring & Privacy) by their line manager as part of their local induction.

2.2 Passwords

ADVICE:

You should select a password that cannot be easily guessed.

Most passwords are CASE SENSITIVE.

Computer screens can be locked by pressing the keys **Ctrl, Alt, Delete** together, and then Enter.

The IT Service Desk will restrict access to all PCs via secure password authentication

You must never leave any PC unattended without activating password protection (either by logging out or locking the computer screen).

Users should not add additional password or security measures to any PC without first consulting with the IT Service Desk.

You are accountable for any information accessed whist logged onto your user account.

Please refer to the PCT's Intranet for more guidance on choosing passwords:

http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm

2.3 Password Sharing

ADVICE:

Using another person's username/password may be a breach of the Computer Misuse Act, 1990.

You can change your password by pressing the keys **Ctrl, Alt, Delete** together, and then selecting the "Change a password" option.

You should not write down your password and should treat it with the same degree of confidentiality as your bank PIN number.

Your network account is issued for your personal use only and must not be shared with anyone, including IT staff. This is for your own protection.

If a breach of security is recorded under a username, the burden of proof will be with the owner of that username to show that they are not responsible for the breach.

If you believe, or suspect that any other user is aware of your personal password you must change the password immediately and if you have any concerns that your password security has been compromised, please inform the IT Service Desk.

2.4 Additional Systems Access

ADVICE:

Access to such systems will require additional written authorisation.

Access to databases or other IT systems (e.g. SBS) containing important and confidential information, will be restricted to those staff who require access as part of their job function.

If you need access, please contact the IT Service Desk for further information.

3 Confidentiality

ADVICE

Document files stored in a user's personal area are only available to that user.

If another member of staff needs access to your work then you should store the information in an area that you can both access.

All staff are responsible for ensuring that sensitive information is used, stored and transferred securely. Sensitive information includes, but is not restricted to personal, patient-identifiable, financial, HR and commercially sensitive information

Sensitive information must be protected in line with the PCT's Information Governance & IT policies and associated guidance at:

http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/docs/GuidelinesPolicies/5-8%20-%20MINIMUM%20SECURITY%20MEASURES%20MATRIX%20v2.pdf

Everyone working with or using personal information has a responsibility to ensure appropriate confidentiality is maintained. Any IT equipment that holds information and is taken off site **must be encrypted** in accordance with the terms of the PCT's *Mobile Computing Procedures and Encryption Policy.*

The PCT is registered for systems in connection with healthcare and its administration under the Data Protection Act 1998.

The use of electronically-held sensitive information at home or from a remote location should be agreed as appropriate under the terms of the *Mobile Computing Procedures*. This is to ensure that

everyone is working in accordance with the PCT's Data Protection Act Notification.

Users are bound by IT security policies and procedures of the PCT.

ADVICE:

You must sign up to the PCT's Internet and E-mail Policy before you are allowed access to the Internet and E-mail services.

Your Line Manager will ensure you do this as part of your local induction.

4 Using E-mail & the Internet

The PCT has an *E-mail and Internet Policy* that can be found on the PCT's Intranet site. This gives detailed information on appropriate use of e-mail and the Internet in the PCT.

For further information, the PCT's E-mail and Internet Policy is available on the PCT Intranet.

5 Privacy of Documents

ADVICE:

The privacy of the messages you receive and the files you create are established by your logon password.

A copy of every document stored on PCT systems is backed up by the IM&T Department. These may be used to recover from system failure, accidental deletion, for court purposes, or investigation of unlawful acts or system misuse.

Information archived may include a copy of every e-mail sent and received plus a full history of all Internet access made, listed by each site visited and the user accessing them.

6 Disclosure

ADVICE:

Access to your e-mail could be granted to others during periods of absence.

Access to interrogate the document archives will only be granted to staff responsible for investigating system failure or system misuse and then only to look at information as necessary to repair or protect the systems or to investigate misuse.

Document files, web browsing logs, e-mail or voicemail messages, however confidential or damaging, may have to be disclosed in court proceedings or during internal investigations.

Access to a user's personal documents or e-mails will only be granted to another user if a written request, with appropriate reasons, is received from the appropriate Senior Manager after consultation with the HR Department. For further guidance please contact the IT Service Desk.

Note that staff may be required to disclose information to the PCT's Freedom of Information Officer in response to Freedom of Information (FOI) requests. For more information on FOI see the PCT Intranet.

7 Copyright

ADVICE:

NHS Corporate Identity Guidelines are available from the PCT Communications Department.

Do not infringe copyright by copying or transmitting copyrighted material without permission of the copyright holder.

The NHS North Yorkshire & York logo must be used only for official PCT documents and in accordance with NHS Corporate Identity guidelines.

8 Data Security and Backups

ADVICE:

A shared area allows a group of staff to share computer files.

Contact the IT Service desk if you need help understanding which shared areas are available.

You should not use the C drive (or any local hard disk) on any computer to store any information. Loss or theft of a PC with sensitive data on it's local hard drive would constitute a serious security breach.

Files on local PC's are not encrypted or backed up – therefore it is essential that you only use PCT file servers for storing your work. The PCT servers are automatically backed up every night. Under exceptional circumstances files can be restored from network servers on an individual basis on receipt of an e-mail request to the IT Service Desk with appropriate justification from your line manager.

9 Dormant Accounts

User accounts identified as not being used for **3 months** will be suspended under the assumption that the employee has left the organisation.

If you change job role you should ensure that your Line Manager has notified the IT Service Desk to ensure your file and system access has been amended appropriately.

If you change job role you should ensure all relevant files and e-mail messages are available to your line manager before moving.

10 Leaving PCT Employment

ADVICE:

It is essential that the Manager informs the IT Service Desk when staff are leaving or have left the PCT.

If a member of staff leaves the PCT, it is the responsibility of their Line Manager to contact the IT Service Desk before they leave, to ensure that all computer files and e-mail messages are dealt with appropriately.

When informed by the HR department or applicable Line Manager that a member of staff has ceased employment, the IT Service Desk will disable the e-mail and login accounts of that staff member.

ADVICE:

Unauthorised connections constitute a serious security risk.

Any unauthorised connection or equipment found will be automatically removed without notice.

If you are aware of any 3rd parties connecting or attempting to connect to the PCT network, please inform the IT Service Desk.

11 Equipment Connections

Do not connect any device (PC, mobile IT equipment, mobile phone, MP3 player, printer, etc) to the PCT Network or a PCT owned PC unless authorised. It is possible to connect devices for the purposes of charging batteries, but not to connect to a PCT asset to gain access to information or applications.

Further guidance on this can be found in the PCT's *Mobile Computing Procedure*.

ADVICE:

Users can assume that equipment that is connected on their behalf by members of the IM&T Department will be compliant with these Acceptable Use Guidelines.

12 Use of PCT IT Equipment

The PCT provides IT equipment that is configured for use in your employment, therefore users should not modify any of the settings on IT equipment other than those routinely required for work purposes. Where the PCT provides a standardised desktop background and screen saver, this must not be altered.

13 Taking Mobile IT Equipment Off-Site

Portable IT equipment provided by the PCT is subject to the same conditions of use whether used at home or in the office.

Users must take all reasonable care and precautions to ensure safe transportation and storage when moving equipment between home or other remote locations, and work.

For further information, and details of the reporting procedure for lost, stolen or damaged equipment please see the PCT's *Mobile Computing Procedure*.

14 Remote Assistance

ADVICE:

This software is used for the purpose of troubleshooting hardware and software problems from a remote location (saving significant travel costs).

Remote assistance software is used by the IM&T Department to connect to and take control of NYY connected and owned PCs remotely to enable IT staff to fix a problem.

IM&T staff will not use this to connect to a PC without first seeking permission of the user of the machine.

Remote assistance will not be given for other purposes, such as allowing managers to monitor their staff's work.

Staff should not attempt to use, install or modify any remote assistance software on any PCT computer.

15 Virus Protection

The PCT network is protected by Anti-virus software but caution should be exercised when opening files from external sources.

To protect the PCT from computer viruses, virus-scanning is enabled on every PC that is connected to the PCT network and all emails are scanned automatically. No document or file from **any source** outside the PCT should be used / opened unless it has been scanned for known viruses. Manual scanning is also possible.

Should you receive a virus warning message from a friend or colleague via e-mail, do not forward it on to others, instead send it to the IT Service Desk to determine the authenticity of the warning. These are very often hoaxes and well-meaning people simply propagate them, using up valuable system resources doing so.

If you receive a suspicious attachment via e-mail do not open it – these often contain viruses. Please report any suspicious e-mail messages to the IT Service Desk.

16 Licensing

16.1 Installing or Upgrading Software

All software must be **purchased, installed and configured** in conjunction with the IT Service Desk; this includes all software packages, software upgrades, patches, and add-ons, however minor. All requests for software must be made through the IT Equipment & Software Request form (see Appendix A of the 'IT Funding Procedure').

ADVICE:

The software installed on your PC is licensed for your use.

Violation of a software licence could result in prosecution by FAST (Federation Against Software Theft).

Standard software is purchased centrally by the IT Dept. Non-standard approved software is purchased though departmental budgets. Prior to purchasing this software, approval must be obtained to ensure compliance with Data Quality, Information Governance and compatibility with the IT infrastructure.

Software licensing will be arranged and recorded by the IT Service Desk as part of the procurement and /or installation process.

16.2 Using Software

Software must be used in accordance with the software publisher's licence agreement.

Do not violate licensing agreements by making illegal copies of PCT software.

Any unlicensed software found on a PCT PC will be automatically deleted or disabled and the user could face disciplinary proceedings.

17 Purchasing/Upgrading Equipment

17.1 Purchasing New Equipment/Software

ADVICE:

The IM&T Department will be happy to advise on the purchasing of IT equipment/software and will arrange quotations and orders on your behalf.

In order to ensure that NHS standards are met requests for any computing purchase, from any PCT budget, must be submitted to the IT Service Desk for approval. This applies to orders for hardware, software or IT services. All requests must be submitted on an IM&T Equipment Request Form in accordance with the PCT's *IT Procurement procedure.*

18 Donated or Transferred Equipment

All computers, printers and ancillary equipment used within the PCT must meet IT standards. You should consult with the IT Service desk before accepting any donated equipment.

Any donated equipment will become property of the PCT and may require electrical safety testing before use.

19 Installing Equipment

All computers, printers, mobile IT equipment and ancillary equipment must be installed in conjunction with the Informatics Department.

20 Moving Equipment

No IT Desktop equipment should be moved from its current location without prior agreement and in conjunction with the IT Service Desk.

21 Disposal of Equipment

Redundant IT equipment must only be disposed of through the IT Service Desk, who will arrange for secure disposal in accordance with the EU Directive on Waste Electrical and Electronic Equipment (WEEE), PCT policy and Information Governance Good Practice.

22 General Misuse

22.1 Prohibited Activities

PCT equipment must not be used for the creation, transmission or deliberate reception of any images, data or other material, which is designed or likely to cause offence or needless anxiety, or is abusive, sexist, racist, defamatory, obscene or indecent.

When communicating electronically, staff are expected to conduct themselves in an honest, courteous and professional manner.

PCT resources, including printers, must not be used for private work or commercial gain.

Staff can not use the PCT's IT facilities for commercial activities; this includes but is not limited to advertising or running any sort of private business.

Staff can not use the PCT's IT facilities for Advertising or Fund-raising for commercial or charitable organisations not directly connected with the PCT.

It is the responsibility of all staff within the PCT to ensure that computer systems and the data that is accessed through them, are safe and secure. Staff who have an e-mail account have additional responsibilities relating to security, confidentiality and appropriate use.

Any breaches should be reported immediately to the IT Service Desk and Network & Development Manager, who will assist the user to ensure that the incident is logged via the Trust incident reporting system. Any major IT incidents or 'near misses' (defined here as an activity or action with the *potential for* causing a security breach or incident) will be reported via an incident report as soon as possible. A major incident would constitute a loss of function of a clinical system or breach of confidential information for one or more individuals or a breach of information which is likely to lead to harm to an individual.

23 Compliance with these Guidelines

The guidelines and warnings listed within this document and associated documents are of critical importance, and non-compliance could in certain circumstances constitute a serious disciplinary matter.

Any breach of the policies signposted within this policy may be subject to disciplinary action.

Any concerns around compliance with these guidelines should be discussed with your line manager.