

**E-Mail & Internet**

**Acceptable Use**

**Policy**

**April 2005**

## AMMENDMENT HISTORY

Version	Status	Date	Comments	Author
X	Written	May 03	First ideas	A Jones
Y	Update	Sep 03	From Feedback	A Jones
Draft	Update	Jan 04	Security added	A Jones
Draft A	Update	Feb 04	Simplification	A Jones
Daft B	Update	Jan 05	From Feedback	A Jones
1	Update	Apr 05	From Software Audit	A.Jones

Approved By:	B. Wood Head of IT Shared Services	Signature: Date: March 2005
	Information Governance Group	Signature: Date March 2005
	GPT Board	Signature: Date: March 2005

## CONTENTS

1. Introduction .....	3
2. Security Policy.....	4
3. Appropriate Use of Email Policy.....	5
4. Unacceptable use of Email & Internet Policy.....	7
5. Virus Checking Policy.....	9

## 1. INTRODUCTION

### Why an Acceptable Use policy?

The purpose of this Acceptable Use Policy (AUP) is to make all staff aware of their roles and responsibilities for Information Security when handling information confidential to the NHS organisations in the County and Patient Identifiable Information (PID).

### Acceptable Use

This AUP defines the policy to use when accessing Email and the Internet through the local county IT network, supported by the IT Shared Services team for the PT & PCTs, which is connected to the *NHSnet*.

### How to use

Please read through the various sections in order as they introduce you to concepts that may be new to you and appropriate ways to work to get the best out of your use of Email and Internet access.

### Software Licensing

Staff must **NOT** download software from the Internet for use on Trust owned computers without authorisation from the IT Shared Services Helpdesk. This includes shareware, trial and demo software. Only licensed software to be used on Trust owned computers.

### Internet Access Control

For various reasons not all websites are accessible. The controls in place are documented in the IT operational procedure ***C17: Internet Access Controls***.

### Any problems?

If you have any problems in the use of Email or Internet access, please contact the PT & PCT IT Shared Services Helpdesk on Ext. 1025 (Outside – 01452 891025).

## 2. SECURITY POLICY

Access to the Internet for network connected PC's will only be through the Gloucestershire Partnership NHS Trust IT Shared Services NHSnet connection.

Any user is permitted to have standalone (i.e. not connected to the county network), PC access to the Internet through a modem.

### Responsibilities of the User

It is the responsibility of all staff within the NHS establishment to ensure that IT systems and the data which is accessed through them are safe and secure. Staffs that are authorised to access the Internet have additional responsibilities relating to security, confidentiality and appropriate use as below.

### Permissible Access

Access to the Internet is primarily for Healthcare related purposes. That is for NHS organisations work or for professional development and training. Reasonable personal use is permitted provided this does not interfere with the performance of your duties. Personal access to the Internet can be limited or denied by your local manager. Staff must act in accordance with their manager's local guidelines. Your local NHS organisation has the final decision on deciding what constitutes excessive use.

### Non-Permissible Access

No member of staff is permitted to access, display or download from Internet sites that hold offensive material. Doing so is considered a serious breach of NHS organisations security and may result in dismissal or prosecution. Offensive material is defined by the 'Managing Opportunity' and 'Harassment & Bullying' Policies and includes hostile text or images relating to gender, ethnicity, race, violence, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive and includes Internet and e-mail. Other than instances which demand criminal prosecution, the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet will be decided by senior NHS management.

### Management of Security

The overall responsibility for maintaining the Partnership Trust security policy lies with the organisation Information Security Officer.

The Head of IT Services (PT & PCT), has the responsibility for the protection of IM&T assets within the Gloucestershire Partnership NHS Trust and PCTs (and supported GP practices) within the County.

The PT & PCT IT Shared Services Network Security Manager is the first point of contact for clarification of security issues and can be contacted via IT Shared Services Helpdesk on 01452 891025.

### 3. APPROPRIATE USE OF EMAIL POLICY

#### 3.1 General Rules:

1. The only email system that lets you send confidential or patient identifiable information is the National NHS Contact email service. This is achieved by encrypting emails between NHS Contact email users **ONLY**. The local Email Messaging System does **NOT** encrypt messages while in transit.
2. The IT Shared Service local Email Messaging System and National NHS Contact email service are primarily for business use. Occasional and reasonable personal use is normally permitted provided that this does not interfere with the performance of your duties.
3. All email is stored centrally and the IT Shared Service may inspect email (including personal email) without notice. Managers must ensure that staff members are aware that the organisation owns the documents they or their colleagues create, nor do they have intellectual property rights therein.

#### 3.2 Email Do's and Don'ts

##### DO

- Check your email regularly each working day or arrange for a duly authorised person to do so on your behalf by use of facilities within your email client software.
- Advise people when you are not available. When out of the office, and not able to log into your mail account, use the tools within your system to notify others of your inability to read your mail.
- Ask yourself before sending an email, how would you feel if your message were read out in court. Email messages may have to be disclosed in litigation.
- Be selective about who receives your -mails, especially when using "Reply to All". Do all recipients need to see the reply?
- Obtain confirmation of receipt for important emails sent.
- Print only when necessary, only making and keeping hard copies of important emails sent and received.
- Keep all passwords secure.
- Reply promptly to all email messages requiring a reply. Where a prompt detailed response is not possible, send a short email acknowledging receipt and giving an estimate of when a detailed response will/should be sent.
- Report to your line manager any email received by you which may be regarded as illegal or offensive.
- Use distribution lists with care. Is it important that all addressees receive the mail?
- Use organisation-wide distribution lists only to communicate important business information that has genuine site wide value.
- Keep the amount of email in your Inbox to a minimum.
- Delete or archive emails when they are no longer likely to be useful.
- If you have a lot of email correspondence, you can make suitable folders in your email client, use the tools provided and/or move emails into folders corresponding to particular activities. However, email systems are not a substitute for a filing system, and the email system places limits on the amount of storage space available to each user. It is better to store most emails and attachments on a network fileserver.
- Recognise that emails with attachments take up valuable space on the computer. Detach

files, file accordingly, and delete the email, if appropriate.

- Use the subject field with a few short descriptive words to indicate the content. It will assist the recipient in prioritising opening of emails and aids future retrieval.
- Be careful about content - email is easily forwarded.
- Maintain the conventions normally used in sending a letter by post. Emails carry the same etiquette as traditional communication.
- If you are receiving a lot of 'Junk mail' or 'inappropriate mail' please contact the IT Shared Services as they may be able to help.

### **DON'T**

- Don't create email congestion by sending trivial messages or personal messages or by copying emails to those who do not need to see them.
- Don't import any non-text file, including files received as email attachments, onto your system without checking them for viruses, using the approved software.
- Don't impersonate any other person when using email or amend messages received.
- Don't be caught out by the speed of email. Do not act impetuously. Is your first reaction the one you want the recipient to receive?
- Don't verbally attack in electronic form.
- Don't send email in upper case - this is the equivalent of shouting at someone.
- Don't send emails to lots of people just because you can.

## 4. UNACCEPTABLE USE OF EMAIL & INTERNET POLICY

The following is a list which is appropriate to both email use and Internet use – remember some uses are illegal not just unacceptable by the NHSIA, *NHSnet* and NHS organisations.

Email and Internet access must **NOT** be used for any of the following:

1. the creation or transmission (other than properly supervised and lawful clinical purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
3. the creation or transmission of defamatory material;
4. the transmission of material such that this infringes the copyright of another person;
5. the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks;
6. Non-Healthcare Profit making activity that abuses the service;
7. other activities that do not benefit patient care or that do not support the professional concerns of those providing that care, where those activities constitute abuse of the service;
8. abuse of the service by the unsolicited sending of inappropriate email to large numbers of people, whether on *NHSnet* or on the Internet;
9. deliberate unauthorised access to facilities or services accessible via *NHSnet*;
10. deliberate activities with any of the following characteristics:
  - flagrant wasting of staff effort or networked resources, including time on end systems accessible via *NHSnet* and the effort of staff involved in the support of those systems;
  - corrupting or destroying other users' data;
  - violating the privacy of other users;
  - disrupting the work of other users;
  - using *NHSnet* in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
  - continuing to use an item of networking software or hardware after the NHS Information Authority – Access Services has requested that use cease because it is causing disruption to the correct functioning of *NHSnet*;
  - other misuse of networked resources, such as the introduction of “viruses”;
  - where *NHSnet* is being used to access another network, or any abuse of the acceptable use policy of that network will be regarded as unacceptable use of *NHSnet*.
11. excessive sending and receiving of private emails particularly where these contain pictures;

12. note that this list is not exhaustive, and will be updated in the light of experience.
13. Use of File Sharing services for the sharing of music, videos, pictures and software.
  - The PT & PCT IT Shared Services does not consider these services necessary for normal NHS organisations business needs.
  - You should not use those services which could compromise the security of the IT Shared Services network.
  - If you have a valid NHS business need to use a specific file sharing service please discuss with the IT Shared Services team so that appropriate security measures can be put in place.
14. Staff must not download software for use on Trust owned computers without authorisation from the IT Shared Services Helpdesk. This includes shareware, trial and demo software. Only licensed software to be used on Trust owned computers.

## 5. VIRUS CHECKING POLICY

### 5.1 Introduction

As Viruses and other malicious software use Email services and can be hidden in files downloaded from the Internet or other organisations, the following is the policy of how to ensure that what you do will reduce the risk of spreading Viruses. If you suspect that the anti-virus checking software on your PC is not working or is out of date, contact the IT Shared Services Help Desk who will arrange for it to be checked.

### 5.2 Emails & Attachments

In utilising e-mail to send /receive information in the form of attachments or encrypted files, the following points need to be adhered to:

- Treat all attachments with caution.
- Do not view/open any attachments which have been sent by someone you do not know.
- Do not open any suspicious e-mails you receive from unknown organisations or persons – to be safe delete without opening plus remember to delete from the wastebasket. Remember that e-mail is a direct derivative of the Internet.
- Should you receive any virus warning messages other than from the IT Shared Services team, please contact the IT Shared Services Help Desk before you forward them to all your colleagues.
- Do not leave your workstation unattended while logged in and connected to a network session. This could allow unauthorised e-mails being sent in your name and allow someone to access files using your credentials.

### 5.3 Downloaded Files

When downloading files from the Internet, the following points need to be adhered to:

- Treat all downloaded files with caution.
- Do not view/open any file which you are not sure of, from someone you do not know.
- Do not open any files from unknown organisations or persons
- Remember that no shareware, trial or demo software to be installed on Trust computers without authorisation from the IT Shared Services Helpdesk. Only licensed software to be used on Trust owned computers.

