Notice:

Plymouth Community Healthcare Community Interest Company adopted all Provider policies from NHS Plymouth when it became a new organisation on 1 October 2011.

Please note that policies will be reviewed to reflect the new organisation in line with the reader information sheet, or sooner where this is possible.

NHS Plymouth

Use of Email Policy

Version No 3:6

Notice to staff using a paper copy of this guidance

The policies and procedures page of Healthnet holds the most recent and approved version of this guidance. Staff must ensure they are using the most recent guidance.

Authors/Editor	Business Development Manager
Access ID Number	19

Reader Information and Asset Registration

Title	Use of Email Policy v3:6
Information Asset Register Number	PPCTG19
Rights of Access	Public
Type of Formal Paper	Policy
Category (Please identify type)	Corporate
Format	Word Document
Language	English
Subject	Use of Email
Document Purpose and Description	The Trust wishes to actively encourage and promote the responsible use of electronic communications in the administrative, business and technical operations of the Trust. This policy is for all staff that use or intend to use email
Author(s)/Editor(s)	T. Daniel, Information Security Manager
Ratification Date and Group	May 2010 - ISGC
Publication Date	29/06/2012
Review Date and Frequency of Review	17/11/2012 2 yearly
Disposal Date	The Public Information Service will retain a copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or has been withdrawn from circulation.
Job Title of Person Responsible for Review	Information Security Manager
Target Audience	All staff that use or intend to use email.
Circulation List	Electronic: Via Healthnet Via PCT website (subject to Freedom of information exemptions) Written: Upon request to the Public Information Service on ☏ 01752 272511 Please note this document can be made available in other formats if required please contact the Public Information Service on ☏ (01752) 272511
Consultation Process	Nil.
Equality Impact Assessment and Human Rights Assessment	No
References/Source	• The Common Law Obligation of Confidentiality • The Data Protection Act 1998 • The Computer Misuse Act 1990

	• The Access to Health Records Act 1990 • The Copyright, Designs and Patents Act 1988 • The Public Records Act 1958/1967 • The Human Rights Act 1998 • The Crime and Disorder Act 1998 • The Regulation of Investigatory Powers Act 2000 • The Freedom of Information Act 2000 • The Caldicott Committee Report on the Review of Patient-Identifiable Information Report • NHS IM&T Security Manual – NHS Information Authority • BS7799 • The Protection and Use of Patient Information – Department of Health • For the Record' - The Management of Health Records – Department of Health • NHSnet Networking Security Policy and Code of Connection – NHS Information Authority
Supersedes Document	Use of Email Policy v3:5
Author Contact Details	Business Development Manager
Publisher: (for externally produced information)	

Document Version Control

Version Number	Details e.g. Updated or full review	Date	Author of Change	Description of Changes and reason for change
V.2	Full review	26/8/2005	T Daniel/ S Edmunds	Full content and layout changes
V 3:0	Updated	13/9/2005	S Edmunds	Minor amendments to reflect new guidance template and note issued by the Use of Information Group.
V3:1	Updated	?	?	?
V3:2	Updated	29/08/2007	L Stanton	Formatted to bring in line with corporate standards
3:3	Reviewed	03/11/2009	T Maclennan	Reviewed, no changes made.
V3.4	Updated	26/01/09	T Maclennan	Minor amendments to reflect sharing of patient identifiable data.

V3.5	Updated	21/06/10	T Seedhouse	Amended to include instructions for clinicians emailing service users
	Changes agreed	26/07/10	ISGC	Committee approval of above changes
V3:6	Review	29/06/2012	PRG	Review date extended, no other changes made.

Contents

Abbreviations	
ICT	Information, Communication and Technology
PICTS	Plymouth Information, Communication and Technology Service

Use of Email Policy

1. Introduction

NHS Plymouth wishes to actively encourage and promote the responsible use of electronic communications in the administrative, business and technical operations of the Trust. Further more it is Trust Policy to protect the privacy of data, users and the security and reliability of Trust systems and networks. This policy relates only to the use of the NHS Plymouth provided email service (XXX@plymouth.nhs.uk).

1.1 The need for an E-mail Policy

This purpose of this policy is to ensure the proper use of the NHS Plymouth email service and to make users aware of what NHS Plymouth deems as acceptable and unacceptable use of its' email service.

NHS Plymouth maintains the right to monitor electronic messages or other electronic files created by users but only in specific instances for which there is good cause.

Where a confidential e-mail is received, care should be taken when forwarding it, to ensure that it is appropriate so to do.

Owners of data are responsible for classifying their data and protecting it to the appropriate level of security / confidentiality before sending it by e-mail. Under no circumstances is patient identifiable data to be sent to addresses other than those internal mail servers eg xxx@plymouth.nhs.uk or unless using a xxx@nhs.net account and have referred to section 9.

2. Legal Risks

Email is a business tool and users are obliged to use this tool in a responsible effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply.

- If you send or forward any emails with any libellous, defamatory, racist or obscene remarks **you** and your Trust can be held liable.
- If you unlawfully send or forward confidential information **you** can be held liable under the data protection act.
- If you unlawfully forward or copy messages without permission **you** can be held liable for copyright infringement.
- If you send a virus or file containing a virus **you** can be held liable.

3. Legal Requirements

The following rules are required by law and are to be strictly adhered to:

- **It is strictly prohibited to send or forward emails containing libellous, defamatory, offensive racist or obscene remarks**.
- Do not send forged or attempt to forge email messages
- Do not send email from another persons email account
- Do not disguise or attempt to disguise your identity when sending mail
- Emails may be subject to disclosure under the Freedom of Information Act 2000.
- Where an email constitutes a corporate record it must be filed with the relevant records and not kept in an individual's mailbox

4. Best Practice

- Do not be caught out by the speed of email - acting impetuously may not be appropriate.
- Do not send unnecessary attachments - use shortcuts where possible
- Always enter a suitable description in the subject line
- Do not write EMAILS IN CAPITALS this is considered as SHOUTING**.**
- Delete emails that you do not need to retain
- Do not forward chain emails.
- When receiving emails beware of the possibility of receiving viruses and ensure that your antiviral precautions are up-to-date
- When sending large attachments the documents should be compressed using suitable software
- Do not send patient identifiable information unless you have made reference to the table of confidential exchange (section 9).

5. User Responsibility Acceptable Use

a. It is the responsibility of the user to ensure that the identity of the Recipient to whom they are sending an email is correct.

b. The User shall ensure that should it be necessary for Patient Identifiable Data to be transferred through the Email Service those obligations details in Section 9 below are adhered to.

c. The User shall not use the email service to violate the laws and regulations of the United Kingdom. Use of this service for illegal activity is grounds for immediate dismissal, and the NHS Plymouth will, without exception, always refer any such incidents to the police. Illegal activity includes (but is not limited to) material related to paedophilia, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Suspicion of such activity may be referred to the appropriate body for their investigation.

d. The User shall not send defamatory material by email, or send communications which knowingly cause distress or offence to another user, or transmit any files of an obscene or pornographic nature. The transmission of any kind of sexually explicit image or document using this service is expressly forbidden. If you need to transmit sexually explicit images or documents for a valid clinical reason, then you shall obtain the permission of the local Caldicott Guardian and inform the

Information Security Team that you intend to use the email system for this purpose before you start doing so.

e. The User shall not attempt to introduce computer viruses via email messages or attachments. The deliberate or negligent transmission or propagation of, without limitation, any virus, worm, "Trojan", trap-door or other malware programme code using this service is expressly forbidden. NHS Connecting for Health will seek reasonable reparation through your local Trust or employing organisation in the event that any of your activity causes any detriment or loss of any kind to the national network service.

f. The User has a responsibility to reasonably understand copyright, trade-mark, libel, slander and public speech control laws, so that the User's use of the email service does not inadvertently violate any laws which might be enforceable against the NHS, local Trust or organisation.

g. The User shall not attempt to send persistent email communications to an individual or mailing list when, as a result of any complaint, a warning has been issued that further communication are not wanted.

h. The User shall not forward chain mail or other frivolous material.

i. Broadcasting to large distribution lists is resource intensive, and the User shall use such lists sensibly and appropriately. Broadcasting to lists over 200 users within an Organisation may only be set up by Organisation administrators who will assess the suitability of such requests.

6. Personal Use

The Email facility is provided for NHS Plymouth Business but may be used for reasonable private use, however the following guidelines must be adhered to:

- Personal use must not interfere with work
- Personal emails must adhere to the guidelines in this policy
- Personal emails must be kept in a special folder clearly marked private
- The forwarding of chain letters, jokes and junk mail is strictly forbidden
- All messages sent including personal messages will remain property of the Trust

7. System Functionality / Limitations

Users of the NHS Plymouth email service will be bound by the following system restrictions:

- The size of the mailbox will be limited to 100MB.
- The sending of attachments exceeding 3MB will be blocked
- Emails in the Inbox which are marked as unread will be deleted after 3 months
- Email accounts not accessed for 3 months will be suspended
- Email will be subject to filtering using commercial software to enforce policy and reduce the impact of SPAM and or malicious software.

- Where necessary email archive software is available

8. References

- The Common Law Obligation of Confidentiality
- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Access to Health Records Act 1990
- The Copyright, Designs and Patents Act 1988
- The Public Records Act 1958/1967
- The Human Rights Act 1998
- The Crime and Disorder Act 1998
- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Caldicott Committee Report on the Review of Patient-Identifiable Information Report
- NHS IM&T Security Manual – NHS Information Authority
- BS7799
- The Protection and Use of Patient Information – Department of Health

9. Confidential data exchange

THE ONLY SAFE WAY TO EXCHANGE PATIENT IDENTIFIABLE EMAILS TO **EXTERNAL** ORGANISATIONS IS TO USE A **NHS.NET** ACCOUNT– THIS MUST BE SET UP via the IT Helpdesk.

Email	**Email**	**Secure?**
xxx@plymouth.nhs.uk	xxx@plymouth.nhs.uk	SECURE
xxx@plymouth.nhs.uk	xxx@phnt.swest.nhs.uk	SECURE
xxx@nhs.net	xxx@nhs.net	SECURE
xxx@plymouth.nhs.uk	xxx@nhs.net	**NOT SECURE**
xxx@nhs.net	xxx@x.gsi.gov.uk; xxx@gsi.gov.uk; xxx@gse.gov.uk; xxx@gsx.gov.uk; xxx@police.uk; xxx@pnn.police.uk; xxx@cjsm.net; xxx@scn.gov.uk ; xxx@gcsx.gov.uk	SECURE

xxx@plymouth.nhs.uk	xxx@x.gsi.gov.uk; xxx@gsi.gov.uk; xxx@gse.gov.uk; xxx@gsx.gov.uk; xxx@police.uk; xxx@pnn.police.uk; xxx@cjsm.net; xxx@scn.gov.uk ; xxx@gcsx.gov.uk	**NOT SECURE**

Good practice for sending person-identifiable information by e-mail

If person-identifiable information is to be sent by e-mail internally or externally via the nhs.net, it should only be transferred in line with Caldicott Principles and the Data Protection Act.

The Caldicott Principles govern the use of information about service users to ensure that the minimum amount of person-identifiable information is exchanged and only when absolutely necessary.

The Caldicott Principles:

(i) Justify the purpose(s) for using person-identifiable information.

(ii) Only use person-identifiable information when absolutely necessary.

(iii) Use the minimum amount of person-identifiable information that is required and only those items essential to the purpose.

(iv) Access to person-identifiable information should be on a strict need to know basis.

(v) Everyone must understand and be aware of their responsibilities.

(vi) Everyone should understand and comply with the law.

Individuals have a right to see a copy of information held about them at any time under the Data Protection Act and this includes e-mails containing personal information.

Emailing Patients/Service users

It is recognised that email can be an efficient communication method between a clinician and service user. Email should only be used as a form of communication if it has been requested by the patient, in which case the clinician should initially ask the patient to email them thus providing a reply path containing the preferred email address. This will then reduce the risk of the wrong email address being used.

It should be remembered that any correspondence with a patient will form part of the clinical record and as such will be governed by the usual storage and retention controls.

The form in **Appendix1** should be used when emailing patients. The risk associated with emailing patients includes, but is not limited to:

- Email to public internet email addresses (e.g. name@googlemail.com) is not secure at any point.
- An unlocked PC or publically situated PC could result in a confidential email being left open to view.
- The email could be forwarded to another email recipient.
- The email could be sent to the wrong patient, unless an email link is created
- The email could be printed and passed to the wrong person
- If the patient gives you a work email address, this address would usually name the organisation that the person works for.
- A virus could spread this email onto other individuals
- If an attachment is used then a 'cached' copy of this will reside on the PC that the email is opened on (e.g. the patients/service user) and can be accessed by others who have access to this PC
- The patient should be reminded to inform you of any change of email address.

For further information please contact:

Business Development Manager and Information Governance Lead
01752 343992

Annex A

Consultation List

Annex B

Intended distribution list

All staff

The Lead Director approves this document and any attached appendices.

Signed: - ……

Date: - ……

Appendix 1- Emailing patients

Request for NHS Plymouth to contact patient via personal e-mail address.
NHS Plymouth is committed to open working and efficiency in providing services. To ensure that services are as tailor made as possible to the requirements of its patients NHS Plymouth recognises that with advancing technology, current and routine forms of communication may not be convenient or possible with some patients. To this end NHS Plymouth will be willing to undertake e-mail correspondence with the patient under the
following conditions.

- This agreement is entered into at the request of the patient

- The patient understands that NHS Plymouth has no responsibility for information that leaves authorised NHS (National Health Service) networks at the request of the patient and as such cannot guarantee the security of such information

- The patient understands that NHS Plymouth has no responsibility for equipment used by the patient to send or receive e-mail

- The patient has satisfied themselves that access to their own system is secure and are aware of shared e-mail accounts, shared computers etc.,

- To minimise the risk of 'human error' in writing e-mail addresses, the patient will send an e-mail to: _*insert clinicians email address here*_ in the first instance. This will give NHS Plymouth their preferred e-mail contact address and will be used to correspond with them. A test email will be returned by NHS Plymouth to indicate safe receipt and that the sent address will be the one used to correspond with the patient.

- NHS Plymouth reserves the right to terminate this agreement if there is any virus or other such technical threats to its internal systems as a result of external e-mail traffic.

By signing below the patient indicates they have read and understood the conditions given above. The patient also understands they are able to review or cancel this arrangement at any time in writing.

Name _____
Address _____
Signature _____
Agreed on behalf of NHS Plymouth
_____signature