

Acceptable Use of E-mail Policy

To be read with:

- Acceptable Use of the Internet Policy
- Acceptable Use of Information Systems Policy
- Confidentiality and Data Protection Policy
- Safe Haven Policy
- User Accounts Policy
- Performance and Conduct Policy

Version	1.6
Status	Ratified
Author/Lead	Information Governance & Data Protection Officer
Directorate	Finance and Performance
Ratified By	ICT & Information Governance Programme Group
Date Ratified	22 January 2010
Date Issued	05 February 2010
Date of Next Formal Review	21 January 2011
Target Audience	All Staff

“The PCT incorporates and support the human rights of the individual as set out in the European Convention on Human Rights and the Human Rights Act 1998”

Version Control Record

Version	Description of Change(s)	Reason for Change	Author	Date
1.0	Initial Draft		Assistant Director for Health Informatics	29/08/2006
1.1		Review	Business Systems Manager	02/09/2008
1.2	Clarification on the sending of PID via e-mail strengthened.	Annual Review	Information Governance and Data Protection Officer	13/10/2009
1.3	Amendments to E-mail content monitoring	Feedback from Head of ICT	Information Governance and Data Protection Officer	18/11/2009
1.4	Amendments regarding NHSLA compliance	Feedback from Interim Head of Governance	Information Governance and Data Protection Officer	17/12/2009
1.5	Reference to Performance and Conduct Policy	Feedback from Head of Corporate Affairs	Information Governance and Data Protection Officer	17/12/2009
1.6	Changes to Legal Considerations Section	Feedback from ICT & IG Programme Group and ratified pending changes.	Information Governance and Data Protection Officer	22/01/2010

Table of Contents

1.	Introduction	4
2.	Legal Considerations for E-mail	4
3.	Sending Sensitive Personal Information by E-mail.....	5
4.	The Use of E-mail for Personal Purposes	5
5.	Best Practice Guidelines for E-mails	6
6.	Do's and Don'ts.....	7
7.	E-mail Monitoring	8
8.	Access to Staff E-mail	8
9.	Monitoring and Review.....	8
	Appendix 1 - Acceptable Methods for E-mailing Sensitive Personal Information.....	9
	Appendix 2 - Registering for an NHSmail E-mail Account	10
	Appendix 3 - Equality Impact Assessment Toolkit	11
	Appendix 4 - Audit Tool For The Acceptable Use of E-mail Policy	13
	Appendix 5 - Assurance Form	14
	Appendix 6 - Policy Ratification and Publication	15

1. Introduction

- 1.1 This policy outlines the acceptable use of the PCT's and NHSmail e-mail systems. It should be read in conjunction with the PCT's Acceptable Use of Information Systems Policy which sets out the agreed policy for the use of all PCT owned and operated information systems.
- 1.2 The purpose of this policy is to ensure the proper use the PCT's e-mail system and make users aware of what the Organisation deems as acceptable and unacceptable use of its e-mail system.
- 1.3 This policy applies to all employees of the PCT including contracted and temporary staff.
- 1.4 Staff are advised to familiarise themselves fully with this policy and to have due regard for professional behaviour and etiquette when carrying out any type of communication on behalf of the organisation.
- 1.5 Breach of this policy may result in disciplinary under the PCT Performance and Conduct Policy.

2. Legal Considerations for E-mail

- 2.1 E-mail is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner.
- 2.2 Although by its nature e-mail seems to be less formal than other written communication, e-mail is legally attributable to the Trust in exactly the same way as letters/fax/memos. An e-mail should therefore be regarded as a written formal letter.
- 2.3 The content of all e-mail stored on equipment owned by the Trust remains the property of the Trust.
- 2.4 All employees are responsible for maintaining the confidentiality of information and complying with the Caldicott Principles and Data Protection Act.
- 2.5 Patient / person identifiers should be removed wherever possible, and only the minimum necessary information sent.

3. Sending Sensitive Personal Information by E-mail

- 3.1 Normal PCT e-mail (i.e. firstname.lastname@brentpct.nhs.uk) is an insecure system. Therefore, confidential information (i.e. Person/Patient Identifiable Data) MUST NOT be sent to any external e-mail address. Confidential information may only be sent from your normal PCT e-mail account to another Brent PCT e-mail account (i.e. firstname.lastname@brentpct.nhs.uk to firstname.lastname@brentpct.nhs.uk).
- 3.2 NHSmail (www.nhs.net) is the only approved e-mail account for sending confidential information (i.e. Person/Patient Identifiable Data). This is because the NHSmail service encrypts data between NHSmail accounts to standards approved by the NHS. However, it must be remembered that information sent from an NHSmail account is only encrypted when sent to another NHSmail account (i.e. firstname.lastname@nhs.net to firstname.lastname@nhs.net). See Appendix 2 to register for an NHSmail account.
- 3.3 E-mail sent over the internet is not secure and as such it is not acceptable to use your personal e-mail account (i.e. Hotmail, Gmail, Yahoo!, BT Internet, etc.) for any PCT related business. Under no circumstances should Personal Identifiable Data be sent via a personal e-mail account.
- 3.4 There are certain government e-mail addresses that NHSmail accounts (i.e. firstname.lastname@nhs.net) can communicate to securely. Please refer to Appendix 1 for guidance on this.
- 3.5 In summary, the acceptable options for sending person identifiable information by e-mail are:
- From one named individual @brentpct.nhs.uk e-mail account to another named individual e-mail @brentpct.nhs.uk account.
 - From one @nhs.net e-mail account to another @nhs.net or approved government e-mail account.

4. The Use of E-mail for Personal Purposes

- 4.1 Although the PCT's e-mail system is meant for business use, the PCT allows the reasonable use of e-mail for personal use as long as certain guidelines are adhered to:
- Personal use of e-mail should not interfere with work.
 - Personal e-mails must also adhere to the guidelines in this policy.
 - Personal e-mails are kept in a separate folder, named 'Private'. The e-mails in this folder must be deleted weekly so as not to clog up the system.
 - The forwarding of chain letters, junk mail and executables is strictly forbidden.
 - The e-mail systems must not be used for the purposes of commercial advertising.

5. Best Practice Guidelines for E-mails

The PCT considers e-mail as an important means of communication and recognises the importance of proper e-mail content and speedy replies in conveying a professional image and delivering good customer service. Therefore the PCT wishes users to adhere to the following guidelines:

- Write well-structured e-mails and use short, descriptive sentences.
- Particular care should be taken when sending person identifiable or business sensitive information.
- The PCT's e-mail style is informal. This means that sentences can be short and to the point. The use of abbreviations and characters such as smileys however, is not encouraged.
- Use the spell checker before you send out an e-mail.
- Do not send unnecessary attachments.
- Do not write e-mails in capitals. This appears as if you are shouting and is considered rude.
- Do not print e-mails unless you really need to for work purposes. E-mails can be saved, if you need them.
- If you need a reply to your e-mail by a particular date let the recipient know this.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only send e-mails the content of which could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the e-mail, using other means of communication, or protecting information by using a password.
- Avoid using e-mail for sensitive or emotional messages. Re-read messages prior to sending to check for clarity and ensure that they do not contain anything that could embarrass the individual or organisation, or make the organisation liable.
- Only mark e-mails as important if they really are important.
- At all times when you leave your workstation you must 'lock' the workstation to stop other unauthorised individuals gaining access to your e-mail.
- Ensure you send your e-mail only to people who need to see it. Sending e-mails to all in your address book can unnecessarily block the system. Similarly, "Reply to all" should only be used when necessary.
- E-mails should be treated like any other correspondence and should be answered as quickly as possible.
- Delete any e-mail messages that you do not need to have a copy of.
- Be mindful of what you write on e-mails as this can be requested under the Freedom of Information (FOI) Act. See the following for further guidance:
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx
- Do not forward work e-mails from your PCT account to a personal / home e-mail account. When working from home staff should use the PCT's Remote Access Solution to access the PCT's secure network.
- If you suspect you received a virus by e-mail telephone the IT Service Desk (020 8795 6676) immediately.
 - Do not switch off your PC unless told to do so by the IT Service Desk.
 - Do not attempt to remove the virus yourself. The IT Service Desk will need to know what virus it is.

6. Do's and Don'ts

Do

- Register for an NHSmail e-mail account (Appendix 2).
- Think carefully when composing mails, the nature of e-mail is that it is often less formal than letters etc. This informality can cause differences in interpretation amongst recipients.
- Use distribution lists appropriately. Is it important that all addressees receive this e-mail?
- Check your e-mails regularly, and respond to requests promptly.
- Advise people when you are not available by setting 'Out Of Office auto-reply' on the system.
- Be selective about who receives your e-mails, especially when using 'Reply to All'. Do all recipients need to see the reply?
- Refer to the Best Practice Guidelines for E-mails.
- Remember that a mail from a Trust e-mail account reflects on the organisation. It is also admissible in a court of law and may require disclosure under the Freedom of Information Act.
- Manage you mailbox.
- Keep your password secure.

Don't

- Send Person/Patient Identifiable Data by an unapproved method. Refer to Appendix 1 for guidance.
- Do not send or forward e-mails containing libellous, defamatory, offensive, harassing, racist, obscene, illegal or pornographic remarks or depictions. If you receive an e-mail of this nature, you must promptly notify your line manager.
- Do not breach copyright or licensing laws when composing or forwarding e-mails and e-mail attachments.
- Send e-mail messages using another person's e-mail account except where permissions have been granted.
- Forge or attempt to forge e-mail messages.
- Use e-mail to perpetrate any form of fraud or criminal activity.
- Bring the organisation or a colleague into disrepute.
- Forward a confidential or personal message without acquiring permission from the sender first.
- Use the e-mail system for personal gain.
- Send or Forward unsolicited (i.e. junk mail, spam or chain mail) e-mail messages.
- Purposefully Send or Forward an e-mail and/or an attachment that contains a virus.
- Open mail where you do not recognise the sender or the contents appears to be dubious – it may be a virus.
- Open attachments with exe or vbs extensions.
- Automatically forward e-mails to public Internet e-mail addresses.

Remember – Ask if you are in doubt.

7. E-mail Monitoring

7.1 The PCT undertakes the following monitoring activities:

- All e-mails are monitored for viruses. All e-mail traffic (incoming and outgoing) is logged automatically. The logs do not include e-mail content. These logs are audited periodically.
- The content of incoming e-mails are monitored to limit the PCT's exposure to SPAM, inappropriate and offensive material wherever possible.
- Outgoing emails are not routinely monitored. However, The PCT reserves the right to retain and inspect message content as required for legal, statutory and performance / disciplinary purposes.

8. Access to Staff E-mail

Please refer to the User Accounts Policy for guidance on access to staff e-mail.

9. Monitoring and Review

This policy will be reviewed once a year by ICT. Auditing of this document should be done at least every two years based on monitoring the effectiveness of the policy in line with legislation and guidelines etc. An Audit Tool (Appendix 4) or Key Performance Indicator (KPI) will be used for monitoring purposes. The document Assurance Form (Appendix 5) will be used by Managers to document embedding of policies.

Appendix 1 - Acceptable Methods for E-mailing Sensitive Personal Information

	Brent PCT name@brentpct.nhs.uk	NHSmail name@nhs.net	Other NHS Trust Organisations name@barts.nhs.uk or name@uclh.nhs.uk etc...	Education, Government and Police Organisations name@organisation.gsi.gov.uk name@organisation.police.uk name@organisation.pnn.police.uk name@organisation.gse.gov.uk name@organisation.gsx.gov.uk name@organisation.gcsx.gov.uk name@organisation.scn.gov.uk name@organisation.mod.uk name@organisation.cjism.net i.e. name@brent.gov.uk.cjism.net name@cjism.net	Personal Webmail name@hotmail.com or name@yahoo.co.uk etc...
Brent PCT (brentpct.nhs.uk)	√	X	X	X	X
NHSmail (nhs.net)	X	√	X	√	X
Other NHS Trust Organisations (.nhs.uk)	X	X	X	X	X
Education, Government and Police Organisations (cjism.net)	X	√	X	√	X
Personal Webmail	X	X	X	X	X

Appendix 2 - Registering for an NHSmail E-mail Account

1. To sign up for your free NHSmail e-mail address go to <http://www.nhs.net> and click on

 Register here

(Please note, you must use an NHSnet/N3 connected computer to register.)

2. Enter in your 'First Name' and 'Last Name', and click on

 Search

Click on your name.

3. Ensure that you have selected the correct person – Check the organisation assigned to your name. Click on

 Next

4. Read and Accept the "Acceptable Use Policy" by checking



Then click on

 Next

5. Choose an e-mail address by clicking on



Then click on

 Next

6. Complete the on screen instructions by providing 'Security Questions' and 'Security Answers'.

Then click on

 Next

7. Complete the Registration by checking your details and clicking on

 Finish

Appendix 3 - Equality Impact Assessment Toolkit

DOCUMENT AUTHOR	DIRECTORATE
NAME OF DOCUMENT/POLICY/STRATEGY/PROCEDURE	NEW EXISTING ASSOCIATED POLICIES, STRATEGIES OR PROCEDURES
DATE	

Aim/Status

[a] What is the aim/purpose of the policy/strategy/procedure?
[b] Who is intended to benefit from this policy/strategy/procedure and in what way?
[c] How have they been involved in the development of this policy/strategy/procedure?
[d] How does it fit into the broader corporate aims?
[e] What outcomes are intended from this policy/strategy/procedure?
[f] What resource implications are linked to this policy/strategy/procedure?

Impacts

[a] what is the likely impact [whether intended or unintended, positive or negative] of the initiative on individual users or on the public at large?		
[b] Is there likely to be differential impact on any group? If yes, please state if this impact may be adverse and give further details [e.g. which specific groups are affected, in what way, and why you believe this to be the case]		
[i] Grounds of race, ethnicity, colour, nationality or national origin	Please tick box yes <input type="checkbox"/> no <input type="checkbox"/>	Please tick box Adverse? <input type="checkbox"/> Please give further details
[ii] Grounds of sex or marital Status Women and Men	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details

[iii] Grounds of gender: Transgender or Transsexual People	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[iv] Grounds of religion or belief: Religious /faith or other Groups with a recognised belief system	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[v] Grounds of disability	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[vi] Grounds of age: Older people, children and Young people	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[vii] Grounds of sexual orientation: Lesbian, gay, bisexual	Yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[viii] Grounds of carers: Older relatives, children	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[ix] Grounds of human rights	yes <input type="checkbox"/> no <input type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
Is the policy directly discriminatory? yes <input type="checkbox"/> no <input type="checkbox"/>	Is the policy indirectly discriminatory? yes <input type="checkbox"/> no <input type="checkbox"/> If you said yes, is this objectively justifiable or proportionate in meeting a legitimate aim yes <input type="checkbox"/> no <input type="checkbox"/>	Is the policy intended to increase equality of opportunity by permitting positive action or action to redress disadvantage yes <input type="checkbox"/> no <input type="checkbox"/> Please give details.
If the policy is unlawfully discriminatory it must go to a full impact assessment (please Contact the Equality, Diversity & Human Rights Advisor – Human Resources Directorate)		
Persons conducting EqIA		
Signed		Date

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Equality & Diversity Manager together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact the Equality & Diversity Manager.

Appendix 4 - Audit Tool For The Acceptable Use of E-mail Policy

The following are five questions to assess your understanding and implementation of this policy

(Score yourself - Yes or No)

Do you understand the different definition of documents within the policy?	Yes / No
Do you understand the requirement for the main body of a document?	Yes / No
Do you understand the Ratification Process for documents?	Yes / No
Do you understand the Guidance on the Checklist required for writing documents?	Yes / No
Do you understand the process for reviewing / Archiving / consultation and version control?	Yes / No

If you score No for any of the questions, please re read the relevant section of the policy. If you are still unclear please contact the author / service for clarification

A copy of this **should** be kept in your personal file and may be used as part of a continuous profession development folder.

Signed..... **Role**.....

Date.....

Appendix 6 - Policy Ratification and Publication

Policy Title (including version)	Date
Acceptable Use of E-mail Policy 1.6	22 January 2010
Reason for Submission (Please Tick)	
Scheduled Review <input checked="" type="checkbox"/>	New Policy <input type="checkbox"/>
Urgent Amendments <input type="checkbox"/> (Please specify)	Other <input type="checkbox"/>
<input type="text"/>	
Purpose of Policy	
This policy outlines the acceptable use of both the PCT's internal E-mail system and staff use of the NHSmail e-mail system.	
Supporting Evidence Please state list of reviewers/stakeholders and their job title (use a separate sheet if required) along with evidence of their participation in the review/creation of the policy.	
Reviewers: <ul style="list-style-type: none"> • Head of ICT • Head of Corporate Affairs • Head of Governance BCS • Business Systems Manager • Information Governance & Data Protection Officer 	
New Policy: (Please reference sources of Best Practice used, and list applicable legislation)	
N/A	
Reviewed/Amended Policy: (Please provide full details of changes made, reference sources of Best Practice used, and list applicable legislation)	
Sources of Best Practice Used: Model Acceptable Use Policies available on CfH IG Toolkit KnowledgeBase <ul style="list-style-type: none"> • CfH NHSmail Guidance • Policy Development Policy 	
Relevant Legislation: <ul style="list-style-type: none"> • Misuse of Computers Act 1990 • Data Protection Act 1998 	
Amendments: <ul style="list-style-type: none"> • Policy Development Policy format. • Do's and Don'ts • NHSmail / Sensitive Information Guidance • Updated various bullet points in Best Practice section. • Legal Considerations reference Caldicott Principles and Data Protection Act. • All Appendixes. 	
Policy Equality Impact assessed	
TBC	
Policy Approval	

Name:	Mark Easton (CEO), Chair of ICT & IG Programme Group
Signature:	Mark Easton
Date:	05/02/2010
Policy Publication	
Date policy is uploaded on the intranet via the Communications Department	
February 2010	
Policy to be e-mailed to Heads of Services to discuss at team meetings and staff	
TBC	
Policy to be audited annually	
Policy to be audited for compliance in July 2010. Results to be fed back to ICT & IG Programme Group	