

## *Acceptable Use of Information Systems Policy*

<b>Version</b>	2.0
<b>Status</b>	Ratified
<b>Author/Lead</b>	Information Governance & Data Protection Officer
<b>Directorate</b>	Finance and Performance
<b>Ratified By</b>	ICT & Information Governance Programme Group
<b>Implementation Date</b>	03 September 2010
<b>Date of Last Review Date</b>	08 July 2010
<b>Date of Next Review</b>	04 September 2011
<b>Target Audience</b>	All Staff

**To be read with:**

- Information Governance Policy
- Confidentiality and Data Protection Policy
- Bullying and Harassment Policy
- Acceptable Use of Email Policy
- Acceptable Use of The Internet Policy
- Serious Untoward Incident Policy

**“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
0.1	Initial Draft		Helen Morgan	23/08/2006
0.2	Minor changes	Review	Andrew Scheiner	29/08/2006
0.3	Various requested changes from Human Resources incorporated	Review	Andrew Scheiner	08/11/2006
0.4	Minor changes agreed with Human Resources	Review	Andrew Scheiner	15/11/2006
1.0	Assigned approved status and inclusive definition of "employee" inserted	Review	Andrew Scheiner	31/01/2007
1.1	Minor update to reflect Policy Development Policy requirements	Annual Review	Information Governance & Data Protection Officer	20/04/2009
1.2	Amendment to employee use of network. Disciplinary Section added.	Annual Review	Information Governance & Data Protection Officer	21/06/2010
2.0	Comments added from Reviewers	Annual Review and to take into account the Provider/ Commissioning split.	Information Governance & Data Protection Officer	08/07/2010

## Table of Contents

1.	Introduction .....	4
2.	Purpose.....	4
3.	Scope.....	4
4.	Legislation and Guidance.....	4
5.	Definitions .....	5
6.	Responsibilities .....	6
7.	Disciplinary Procedures .....	9
8.	Monitoring and Review.....	9
	Appendix 1 - Equality Impact Assessment Tool.....	10
	Appendix 2 - Audit Tool For The Acceptable Use of Information Systems Policy .....	12
	Appendix 3 - Assurance Form .....	13
	Appendix 4 - Policy Ratification and Publication .....	14

## **1. Introduction**

- 1.1 This policy outlines the acceptable use of the PCT's information systems. By adhering to the guidelines in this policy the user can minimise the potential risks and other harm to the organisation and its stakeholders.

## **2. Purpose**

- 2.1 The purpose of this policy is to ensure the proper use of the NHS Brent's electronic information systems. It specifies what the organisation deems as acceptable and unacceptable use of these systems, and outlines the employer's / systems provider's and the employee's responsibilities towards them.

## **3. Scope**

- 3.1 This policy applies to all employees of NHS Brent and Brent Community Services (BCS), including contracted and temporary staff.
- 3.2 This policy applies to electronic information systems owned and operated by NHS Brent, including systems sited within the premises of independent practitioners, and those hosted externally. This is an overarching policy, and subordinate / local departmental protocols and guidelines will be developed where required.
- 3.3 Paper/manual information systems are covered by the NHS Brent Record Management Strategy.

## **4. Legislation and Guidance**

- 4.1 Principle and Related Legislation:
- Data Protection Act (1998)
  - Copyright Designs and Patents Act (1990)
  - Computer Misuse Act (1990)
  - Freedom of Information Act (2000)
  - Health and Safety at Work Act (1974)
  - Human Rights Act (1998)

## 5. Definitions

### 5.1 Employee

Any individual working for NHS Brent, BCS or a NHS Brent practice and using a NHS Brent funded or supported information system. The designated working status of such individuals includes but is not necessarily be limited to: contractors, employees, locums, non-executive directors, partners, senior partners, secondees, students and work experience placements.

### 5.2 Defamation and Libel

A published (spoken or written) statement or series of statements that is detrimental to the reputation of a person or organisation that is not true can be considered slanderous or libellous and the person towards whom it is made can take legal actions. Please see the Acceptable Use of the Internet Policy for further details.

### 5.3 Bullying and Harassment

Bullying is persistent, offensive, abusive, intimidating, malicious or insulting behaviour that makes the recipient feel upset, threatened, humiliated and vulnerable. Harassment can be a form of discrimination and can take many forms. It is the behaviour of one person that another finds unacceptable, offensive and unwelcome. As well as being physical, bullying and harassment can take more subtle forms in terms of sending or forwarding statements or images including those deemed to be offensive to others and that may prevent an employee from being able to perform in their role effectively. The Trust has a Bullying and Harassment Policy.

### 5.4 Pornography

Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature of email these issues must be taken into consideration. Therefore, NHS Brent defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting.

### 5.5 Copyright

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. A lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. NHS Brent purchases licences on behalf of its users.

## 6. Responsibilities

### 6.1 Chief Executive

The Chief Executive has overall responsibility for ensuring that information systems are used appropriately and in line with Trust policy.

### 6.2 Directors and Line Managers (including practice partners and managers)

It is the line manager's responsibility to ensure that their staff are aware of the policy in relation to the acceptable use of NHS Brent information systems and of any related guidelines or protocols.

Line Managers should ensure that staff are aware of the training on NHS Brent systems that is available and should monitor each staff accordingly.

If a member of staff wishes to access a specific system or open a user account, they must obtain authorisation from their line manager.

### 6.3 Head of ICT

The Head of ICT is responsible for ensuring the security of the Trust's information systems by:

- Ensuring the availability of NHS Brent information systems to users.
- Protecting NHS Brent systems from unauthorised or accidental modification, ensuring the accuracy and completeness of the organisation's assets.
- Protect NHS Brent assets against unauthorised disclosure to preserve the confidentiality of the Trust's information systems.
- Providing controlled access to NHS Brent's information systems to authorised users as requested by their line managers. No unauthorised access to NHS Brent systems or networks by employees, contractors or other third party users is permitted.
- Deleting users accounts when a user is no longer employed by the Trust, on being informed by line management and / or Human Resources.
- Making available to authorised users, appropriate training in the use of PCT information systems.

The Head of ICT is responsible for monitoring user adherence to this policy, where supported by available tools and implemented processes. If there is evidence that a staff member is not adhering to this policy, NHS Brent reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action.

Where system misuse occurs in the PCT or general practice, the Head of ICT reserves the right to limit or withdraw system availability until the cause of the misuse is addressed.

## 6.4

### **Employee**

NHS Brent's information systems and services are provided for the legitimate business purposes of the Trust and Brent practices.

Limited personal use of the systems and services by employees is permitted so long as it does not interfere with the employee's work, or the operation of the Trust's information systems. Personal files must be stored on the employees 'Home Drive' (H:\). **Employees must not store personal music, video or image files to Trust information systems.**

Employees should be aware that the PCT reserves the right to retain and inspect content stored on its information systems as required for legal, statutory and performance / disciplinary purposes.

In the course of their duties, the ICT Service Desk may need to remotely access Trust information systems using software called DameWare. In these instances the ICT Service Desk will ask users that are logged into a PC if they can remotely access their terminal. Once granted, a popup dialogue box will notify users that Service Desk are trying to connect. As with all employees, ICT Service Desk adhere to the same confidentiality rules set out in Trust policy and within employment contracts.

Employees should be aware that the requirements of the NHS Brent Confidentiality and Data Protection Policy are interlinked with this policy particularly in relation to the Disclosure of Information.

Employees have an individual responsibility for ensuring that they attend the relevant training courses which enables them to use information systems effectively. Line Managers will provide information on the training that is available.

Employees must not:

- Allow people who are not authorised users have access to NHS Brent information systems or use an employee's personal login.
- Install software on NHS Brent systems that has not been acquired or procured through NHS Brent's approved processes.
- Store excessive personal files on the PCT's information systems.
- Allow others to copy software or attempt to make changes to or repair computer hardware.
- Interfere with the normal operation of the network or take any steps that substantially hinder others in their use of the network.
- Access files, directories or data, or log onto a computer using a user account which the employee has not been authorised to use.
- Leave computer equipment anywhere where it is at risk of theft, or where unauthorised people may be able to read its contents. If an employee takes equipment out of the office, they must keep it with them at all times, or lock it away securely and out of sight.
- Take away any inappropriate or confidential information if they leave the employment of the Trust.
- Attempt to circumvent any of the legitimate controls in place to govern the acceptable use of information systems.

Employees must:

- Comply with this policy and any other NHS Brent policies relating to information security.
- Report any breach of this policy as soon as they become aware of it, to their line manager.
- Maintain the confidentiality of NHS Brent systems and any data that is stored and password-protect sensitive files.

Employees must also comply with the particular requirements relating to defamation and libel, bullying and harassment, pornography and copyright:

- Defamation and Libel

Employees must not make statements about people or organisations in any document or e-mail that they write, or on any webpage or website, without verifying the basis in fact. Note that forwarding an e-mail with a slanderous or libellous statement also makes the employee liable. Expensive legal action for either NHS Brent or the employee may result if this policy is not followed.

- Bullying and Harassment

Employees must not use a computer or information system to harass other members of staff by sending or forwarding messages or recording content that they might consider offensive or threatening.

Employees perpetrating harassment can also be made subject to NHS Brent's Disciplinary procedure. Any proven case of harassment will result in disciplinary action against the guilty party which could ultimately lead to dismissal. See the Trust's Performance and Conduct Policy for further information.

- Pornography

Employees must not use NHS Brent information systems to send or forward pornographic information to any other person. If an employee receives a file that is pornographic they should report the matter to their line manager. Employees must not download or save pornographic material that has been transmitted to them.

As well as being subject to NHS Brent's own disciplinary procedures, employees can be prosecuted or held liable for possession of, or for transmitting, pornographic material in the UK and elsewhere. In these circumstances, NHS Brent may also be liable for prosecution and may suffer a significant loss of reputation.

- Copyright

Employees must not:

- Alter any software programs, graphics etc without the express permission of the owner.
- Claim someone else's work as their own.
- Send copyright materials by e-mail without the permission of the owner. This is considered copying.

An employee and/or the PCT can face fines and/or up to two years imprisonment for infringing copyright.

## **7. Disciplinary Procedures**

- 7.1 All suspected breaches of this policy will be investigated and may be subject to the Trust's formal disciplinary procedures. Serious breaches may result in immediate suspension and/or termination of contract, under the PCT Performance and Conduct Policy and the Serious Untoward Incident Policy.

## **8. Monitoring and Review**

- 8.1 This policy will be reviewed once a year by the ICT & IG Programme Group. 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 2) will be used for monitoring purposes. The document Assurance Form (Appendix 3) will be used by Managers to document embedding of policies.

## Appendix 1 - Equality Impact Assessment Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

### Summary

<b>Document Author</b>	Information Governance & Data Protection Officer
<b>Directorate</b>	Finance and Performance
<b>Name of Document / Policy / Strategy / Procedure</b>	Acceptable Use of Information Systems Policy
<b>Document Status</b>	New Document <input type="checkbox"/> Existing Document <input checked="" type="checkbox"/>
<b>Associated Policies, Strategies or Procedures</b>	<ul style="list-style-type: none"> <li>• Information Governance Policy</li> <li>• Confidentiality and Data Protection Policy</li> <li>• Bullying and Harassment Policy</li> <li>• Acceptable Use of Email Policy</li> <li>• Acceptable Use of The Internet Policy</li> </ul>
<b>Date</b>	

### 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 checked="" 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 checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[iii] Grounds of gender: Transgender or Transsexual People	Yes <input type="checkbox"/> No <input checked="" 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 checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[v] Grounds of disability	Yes <input type="checkbox"/> No <input checked="" 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 checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[vii] Grounds of sexual orientation: Lesbian, gay, bisexual	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[viii] Grounds of carers: Older relatives, children	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
[ix] Grounds of human rights	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Adverse? <input type="checkbox"/> Please give further details
Is the policy directly discriminatory?  Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	Is the policy indirectly discriminatory? Yes <input type="checkbox"/> No <input checked="" 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 2 - Audit Tool For The Acceptable Use of Information Systems 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 4 - Policy Ratification and Publication

Policy Title (including version)		Date
Acceptable Use of Information Systems 2.0		08/07/2010
Reason for Submission (Please Tick)		
Scheduled Review	<input checked="" type="checkbox"/>	New Policy <input type="checkbox"/>
Urgent Amendments (Please specify)	<input type="checkbox"/>	Other <input type="checkbox"/>
<input type="text"/>		
Purpose of Policy		
This policy outlines the acceptable use of the PCT's information systems.		
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"> <li>• Head of ICT</li> <li>• Business Systems Manager</li> <li>• Information Governance &amp; Data Protection Officer</li> <li>• Service Support Manager</li> <li>• Head of Information (NHS Brent)</li> <li>• Head of Governance (BCS)</li> </ul>		
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: <ul style="list-style-type: none"> <li>• Model Internet Policy available on CfH IG Toolkit KnowledgeBase.</li> <li>• Policy Development Policy.</li> </ul> Amendments: <ul style="list-style-type: none"> <li>• Policy Development Policy format.</li> <li>• Storage of Employee Personal files added.</li> <li>• Disciplinary section added.</li> </ul>		
Policy Equality Impact assessed		
TBC		
Policy Approval		
Name:	Chair of ICT & IG Programme Group	
Signature:		
Date:		
Policy Publication		
Date policy is uploaded on the intranet via the Communications Department		
TBC		
Policy to be e-mailed to Heads of Services to discuss at team meetings and staff		
TBC		
Policy to be audited annually		
TBC - Results to be fed back to ICT & IG Programme Group		