

Information Security Policy

To be read with:

- Information Governance Policy
- Information Risk Policy
- Acceptable Use of Information Systems Policy
- Acceptable Use of E-mail Policy
- Acceptable Use of the Internet Policy

| | |
|-----------------------------------|--|
| Version | 1.2 |
| Status | Ratified |
| Author/Lead | Information Governance & Data Protection Officer |
| Directorate | Finance and Performance |
| Ratified By | ICT & Information Governance Programme Group |
| Date Ratified | 16 March 2010 |
| Date Issued | 17 March 2010 |
| Date of Next Formal Review | March 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 | Version 1.0 document created. | Initial Draft | Business Systems Manager | 15/02/2008 |
| 1.1 | Minor Updates (Policy Pending Full Review): <ul style="list-style-type: none"> - Reference to Brent PCT changed to NHS Brent. - NHS Brent logo added. - USB Flash Drives added to Scope. | Corporate Branding | Information Governance and Data Protection Officer | 24/03/2009 |
| 1.2 | Changes reflect Policy Development Policy requirements. <ul style="list-style-type: none"> - SIRO added to Responsibilities for Information Security. - User Media Section updated. - Reference made to NHS Brent and BCS SIROs. | Annual Review | Information Governance and Data Protection Officer | 11/03/2010 |

Table of Contents

| | | |
|----|---|----|
| 1. | Introduction | 4 |
| 2. | Objectives, Aim and Scope | 4 |
| 3. | Responsibilities for Information Security | 5 |
| 4. | Legislation..... | 6 |
| 5. | Policy Framework..... | 7 |
| 6. | Monitoring and Review..... | 11 |
| | Appendix 1 - Equality Impact Assessment Tool..... | 12 |
| | Appendix 2 - Audit Tool for the Policy Development Policy | 14 |
| | Appendix 3 - Assurance Form | 15 |
| | Appendix 4 - Policy Ratification and Publication | 16 |

1. Introduction

- 1.1 This top-level information security policy is a key component of the PCT's overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.
- 1.2 This policy applies to staff and contractors of NHS Brent, Brent Community Services (BCS) and partner organisations who access NHS Brent information or information systems.

2. Objectives, Aim and Scope

2.1 Objectives

The objectives of the Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets, and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2 Aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications, and networks owned or held by the PCT by:

- Ensuring that staff are aware of and fully comply with relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they will be implemented in the PCT.
- Introducing a consistent approach to security, and ensuring that staff fully understand their own responsibilities.
- Creating and maintaining within the PCT awareness of Information Security as an integral part of the day to day business.
- Protecting information under the control of the PCT

2.3 Scope

This policy applies to all NHS Brent information and information systems including:

- Information collected, processed, stored and communicated by or on behalf of NHS Brent
- Software that is owned or operated by NHS Brent or is used for PCT business
- Websites and the Internet when accessed via the NHS Brent network or when being used for PCT business
- The corporate network and servers that store and process Trust information, whether located within or outside the Trust
- Any device that connects to the corporate servers and network or that accesses Brent information, including PCs, printers, laptops, other portable devices, USB Flash Drives, memory sticks, smart phones, discs and tapes.

3. Responsibilities for Information Security

- 3.1 Ultimate responsibility for information security rests with the Chief Executive of the PCT, but on a day-to-day basis the Technical Services Manager shall be responsible for managing and implementing the policy and related procedures.
- 3.2 The PCT has two Senior Information Risk Owners (SIROs). The Director of Finance and Performance acts as the SIRO for NHS Brent, and the Deputy Director of Finance and Performance acts as the SIRO for BCS. The PCT's SIROs will act as an advocate for information risk for the Board. The SIROs will ensure that identified information security threats are followed up and incidents are managed. The SIROS will also ensure that the Board are kept up to date on all information risk issues.
- 3.3 Line Managers are responsible for ensuring that their permanent, temporary staff and contractors are aware of:-
- Information security policies applicable in their work areas
 - Personal responsibilities for information security
 - How to access advice on information security matters
- 3.3 All staff are required to comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
- 3.5 The Information Security Policy shall be maintained, reviewed, and updated by the Information Governance and Data Protection Officer. This review shall take place annually.
- 3.6 Line managers are individually responsible for the security of their physical environments where information is processed or stored.
- 3.7 Each member of staff is responsible for the operational security of the information systems they use.

- 3.8 All staff are required to comply with the security requirements that are currently in force, and also ensure that the confidentiality, integrity, and availability of the information they use is maintained to the highest standard.
- 3.9 Contracts with external contractors that allow access to the PCT's information systems must be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of external organisations comply with all appropriate security policies.

4. Legislation

- 4.1 NHS Brent is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the PCT, who may be held personally accountable for any breaches of information security for which they may be held responsible. The PCT shall comply with the following legislation and other legislation as appropriate:
- The Data Protection Act (1998)
 - The Data Protection (Processing of Sensitive Personal Data) Order (2000)
 - The Copyright, Designs and Patents Act (1988)
 - The Computer Misuse Act (1990)
 - The Health and Safety at Work Act (1974)
 - Human Rights Act (1998)
 - Regulation of Investigatory Powers Act (2000)
 - Freedom of Information Act (2000)
 - Health & Social Care Act (2008)
 - Children Act (1989 and 2004)

5. Policy Framework

5.1 Management of Security

- At board level, responsibility for Information Security resides with the Director of Finance & Performance.
- The PCT's Security Officer is responsible for implementing, monitoring, documenting, and communicating security requirements for the PCT.

5.2 Information Security Awareness Training

- Information security awareness training will be included in the staff induction process.
- An ongoing awareness programme will be established and maintained to ensure that staff awareness is refreshed and kept up to date.

5.3 Contracts of Employment

- Staff security requirements will be addressed at recruitment stage and all contracts of employment will contain a confidentiality clause.
- Information security expectations of staff will be included within appropriate job definitions.

5.4 Security Control of Assets

Each information asset, (hardware, software, application, or data) will have a named custodian (known as the owner) who will be responsible for the information security of that asset.

5.5 Access Controls

Only authorised personnel who have a justified and approved business need can be given access to restricted areas containing information systems or stored data.

5.6 User Access Controls

Access to information will be restricted to authorised users who have a bona-fide business need to access the information.

5.7 Computer Access Control

Access to computer facilities will be restricted to authorised users who have a business need to use the facilities.

5.8 Application Access Control

Access to data, system utilities, and program source libraries will be controlled and restricted to authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will be dependent upon the availability of a licence from the supplier.

5.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment will be physically protected from threats and environmental hazards.

5.10 Computer and Network Procedures

Management of computers and networks will be controlled through standard documented procedures authorised by the ICT & Information Governance Programme Group.

5.11 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks will be managed on a formal basis. They will be recorded within a baseline risk register and action plans will be put in place to effectively manage those risks. The risk register and all associated actions will be reviewed at regular intervals. Risks relating to information assets will be reported by the Information Asset owner to the appropriate Senior Information Risk Owner. Any implemented information security arrangements shall also be a regularly reviewed feature of the PCT's risk management programme. These reviews will help to identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12 Information Security Events and Weaknesses

All information security events and suspected weaknesses must be reported to the Technical Services Manager. All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events.

5.13 Classification of Sensitive Information

A consistent system for the classification of information within the NHS organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-NHS bodies.

The PCT will implement appropriate information classification controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their NHS information assets.

5.14 Protection from Malicious Software

The PCT will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff are expected to co-operate fully with this policy. Users must not install software on the PCT's property. Users breaching this guidance may be subject to disciplinary action.

5.15 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of The Technical Services Manager before they may be used to transfer data on to the PCT's systems. Such media must also be fully virus checked before being used on the PCT's equipment.

The PCT issues approved USB memory sticks called IronKeys for the transfer of PCT data (including sensitive and Person Identifiable Data). IronKeys incorporate encryption features in line with Department of Health information security and confidentiality guidelines. Users may not in any circumstances use any other USB memory stick.

Users breaching these requirements may be subject to disciplinary action.

5.16 Monitoring System Access and Use

When necessary and as directed by senior management an audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

5.17 Accreditation of Information Systems

The PCT shall ensure that all new information systems, applications, and networks include a security plan and are approved by the Security Officer before they commence operation.

(Organisations are encouraged to develop a series of System Level Security Policies (SLSPs) for systems under their control in order to distinguish between the security management considerations and requirements of each. In this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system. A separate illustrative template will be provided to aid the local development of these SLSPs).

5.18 System Change Control

Changes to information systems, applications, or networks shall be reviewed and approved by the security officer.

5.19 Intellectual Property Rights

The PCT shall ensure that all information products are properly licensed and approved by the security officer. Users shall not install software on the PCT's property without permission from the Technical Services Manager. Users breaching this requirement may be subject to disciplinary action.

5.20 Business Continuity and Disaster Recovery Plans

The PCT will ensure that business impact assessment, business continuity, and disaster recovery plans are produced for all mission critical information, applications, systems, and networks.

5.21 Reporting

The Information Security Officer will keep the Executive Management Team informed of the information security status of the PCT.

5.22 Further Information

Further information and advice on this policy can be obtained from the Service Desk on 020 8795 6676 (servicedesk@brentpct.nhs.uk).

6. Monitoring and Review

6.1 Policy Audit

This policy shall be subject to audit by Internal Audit.

6.2 Disciplinary

Failure to observe the principles set out in this policy may result in disciplinary action in line with the PCT's Performance and Conduct Policy.

6.3 Policy Review

This policy will be reviewed once a year by the ICT & IG Programme Group. Supporting procedures will be audited once a year. 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) or Key Performance Indicator (KPI) 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

| | |
|--|--|
| 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 2 - Audit Tool for the Policy Development 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 |
|---|--|-------------------------------------|
| Information Security Policy 1.2 | | 9 March 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 | | |
| The purpose of this policy is to provide a framework for overall information security management framework for the PCT, and define information security responsibilities. | | |
| 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 • Technical Services Manager • Business Systems Manager • Emergency Planning and Provider Risk Manager • Information Governance and Data Protection Officer | | |
| New Policy: | | |
| (Please reference sources of Best Practice used, and list applicable legislation) | | |
| <ul style="list-style-type: none"> • N/A | | |
| Reviewed/Amended Policy: | | |
| (Please provide full details of changes made, reference sources of Best Practice used, and list applicable legislation) | | |
| <ul style="list-style-type: none"> • Connecting for Health IG Toolkit Guidance Document • NHS Information Security Management Code of Practice | | |
| Policy Equality Impact assessed | | |
| TBC | | |
| Policy Approval | | |
| Name: | Mark Easton (CEO), Chair of ICT & IG Programme Group | |
| Signature: | | |
| Date: | 16 March 2010 | |
| Policy Publication | | |
| Date policy is uploaded on the intranet via the Communications Department | | |
| TBC | | |
| Policy to be emailed to Heads of Services to discuss at team meetings and staff forums (specify date) | | |
| TBC | | |
| Policy to be audited annually (Specify date of audit) | | |
| One year from approval | | |