

## POLICY/PROCEDURE CONTROL SHEET

<b><u>Policy/Procedure Title</u></b>	Information Security Policy		
<b><u>Sponsoring Director:</u></b>	Head of Health Informatics		
<b><u>Implementation Lead:</u></b>			
<b><u>Impact:</u></b>	(a) <i>To patients</i>		<i>None</i>
	(b) <i>To staff</i>		<i>None</i>
	(c) <i>Financial</i>		<i>None</i>
	(d) <i>Other</i>		<i>None</i>
<b><u>Additional Costs:</u></b>	(a) <i>Training: N/A</i>		<i>Budget:</i>
	(b) <i>Implementation: N/A</i>		<i>Budget</i>
	(c) <i>Capital N/A</i>		<i>Budget</i>
	(d) <i>Other N/A</i>		<i>Budget:</i>
<b><u>Training implications:</u></b>			
<b><u>Date of consultation at:</u></b>			
<b><u>Alignment</u></b>	<i>Trust Wide</i>		
<b><u>Date of Final Version:</u></b>			
<b><u>Implementation Date:</u></b>			
<b><u>Date of last review:</u></b>	<i>May 2007</i>		
<b><u>Date of next review:</u></b>	<i>May 2009</i>		
<b><u>Circulation Date:</u></b>			
<b><u>Circulated Staff:</u></b>		Yes	No
	<i>Directors</i>	✓	
	<i>Medical Staff Committee/SMSF</i>		✓
	<i>Records Guardians</i>	✓	
	<i>General Managers</i>	✓	
	<i>H&amp;S Committee Members</i>		✓
	<i>Heads of Department</i>	✓	

## 1. Introduction

The objective of information security is to ensure the confidentiality, integrity and availability of information assets<sup>1</sup>, whilst minimising business damage through the implementation and maintenance of an Information Security Management System (ISMS) meeting the requirement of BS7799-2:1999 'Specification for Information Security Management Systems'.

The purpose of the information security policy is to safeguard the organisation's and patients information within a secure environment and will continue to be developed as standards and best practice are further amended in line with the changing needs of the NHS, the BHNFT and partnership working.

The Chief Executive and the Information Director has approved and supports the information policy.

## 2. Scope of Policy

This policy applies to:

- All Barnsley Hospital NHS Foundation Trusts (BHNFT) information systems and infrastructure.
- All BHNFT employees whilst engaged in work for the BHNFT at any location, on any computer or Internet connection including volunteers, agency, locum and bank staff.
- Any other use by BHNFT employees on any computer or internet connection which identifies the person as a BHNFT employee or which could bring the BHNFT into disrepute.
- Other persons working for the BHNFT, persons engaged on BHNFT business or persons using BHNFT equipment and networks
- All usage by anyone granted access to the BHNFT network

### 2.1. Objectives

The objectives of Information Security Policy are to preserve:

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

---

<sup>1</sup> Information assets are stored physically and electronically, transmitted across networks or telephone lines, sent by fax, spoken in conversations and printed as hardcopy.

## **2.2. Policy 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 BHNFT by:

- 2.2.1. Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- 2.2.2. Describing the principals of security and explaining how they will be implemented in the organisation.
- 2.2.3. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- 2.2.4. Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business. (TIGER)
- 2.2.5. Protecting information assets under the control of the organisation.

## **3. Responsibilities for Security**

- 3.1. Ultimate responsibility for security rests with the Chief Executive of BHNFT but on a day-to-day basis this responsibility is delegated to the Director of Information.
- 3.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-
  - 3.2.1. The information security policies applicable in their work areas
  - 3.2.2. Their personal responsibilities for information security
  - 3.2.3. How to access advice on information security matters
- 3.3. All staff must comply with security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
- 3.4. The Information Security Policy shall be maintained, reviewed and updated by the Information Security Officer in conjunction with the Barnsley Information Governance Group (BIGG). This review shall take place every 2 years.
- 3.5. Line managers shall be individually responsible for the security of their physical environments.
- 3.6. Each user shall be responsible for the operational security of the information systems they use.
- 3.7. Each system user must comply with the security requirements that are currently in force, and must also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- 3.8. Contracts with external contractors that allow access the organisation's information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

## **4. Legislation**

- 4.1.** The Trust 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 Trust, who may be held personally accountable for any breaches of security for which they may be held responsible. The Trust will comply with the following legislation and other legislation as appropriate:

The Data Protection Act (1998)  
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 2000  
Information Security Management Code of Practice

## **5. Policy Framework**

### **5.1. Management of Security**

- 5.1.1. At board level, responsibility for Information Security will reside with the Director of Information.
- 5.1.2. The Trusts Information Security Officer will be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

### **5.2. Information Security Awareness Training**

- 5.2.1. The Information Governance Department is responsible for the delivery of Information Security awareness.
- 5.2.2. Information security awareness training will be included in the staff induction process.
- 5.2.3. An ongoing awareness programme will be established in order to ensure that staff awareness is refreshed and updated as necessary.

### **5.3. Contracts of Employment**

- 5.3.1. Security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.
- 5.3.2. Security Requirements will be included in job definitions.

### **5.4. Security Control of Assets**

Every asset, (hardware, software, application or data) will have a named system manager who will be responsible for the security of that asset.

### **5.5. Access Controls**

Only authorised personnel who have a business need will be given access to restricted areas containing information systems.

### **5.6. User Access Controls**

Access to information will be restricted to authorised users who have a 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 business need to use the applications.

### **5.9. Equipment Security**

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

### **5.10. Computer and Network Procedures**

Management of computers and networks will be controlled by standard procedures that have been authorised by the Head of ICT.

### **5.11. Security Incidents and weaknesses**

All security incidents and weaknesses are to be reported to the Health and Safety Department via the IR1 process. All security incidents will be investigated to establish their cause, operational impact, and business outcome and reviewed at the BIGG.

### **5.12. Protection from Malicious Software**

The Trust will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff will be expected to co-operate fully with this policy. Users are prevented from installing software on the Trust's equipment.

### **5.13. Monitoring System Access and Use**

An audit trail of system access and use will be maintained and reviewed on a regular basis.

### **5.14. Accreditation of Information Systems**

The Trust will ensure that all new information systems, applications and networks include a security plan and are approved by the Change Advisory Board (CAB). Before they commence operation.

### **5.15. System Change Control**

Changes to information systems, applications or networks must be reviewed and approved by the CAB.

### **5.16. Intellectual Property Rights**

The Trust will ensure that all information products are properly licensed and approved by the Head of ICT.

### **5.17. Business Continuity and Disaster Recovery Plans**

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

**5.18. Reporting**

The Information Security Officer will keep the BIGG informed of the information security status of the organisation by means of regular reports.

**5.19. Further Information**

Further information and advice on this policy can be obtained from the Information Governance Department.