

<b>POLICY DOCUMENT CONTROL PAGE</b>	
<b>TITLE</b>	<b>Title: Information Security Policy Manual</b> <b>Version: 1</b> <b>Reference Number: CO12</b>
<b>SUPERSEDES</b>	<b>Supersedes: NA – Version 1</b> <b>Description of Amendment(s):</b>
<b>ORIGINATOR</b>	<b>Originated By: Jenny Wood</b> <b>Designation: Information Security Manager</b>
<b>BOARD AND EXECUTIVE APPROVAL</b>	<b>Referred for approval by: IM&amp;T Strategy Group</b> <b>Date of Referral: 30<sup>th</sup> September 2002</b> <b>Approved by:</b> <b>Approval Date: 9<sup>th</sup> October 2002</b> <b>Executive Director Lead: Director of Nursing and Corporate Development</b>
<b>CIRCULATION</b>	<b>Issue Date:</b> <b>Circulated by:</b> <b>Issued to: Circulation List</b>
<b>REVIEW</b>	<b>Review Date: October 2003</b> <b>Responsibility of: Jenny Wood</b> <b>Designation: Information Security Manager</b>

**POLICY CONTROL PAGE (2) CIRCULATION  
DOCUMENT**

**Circulation List:**

Borough Directors Rochdale, Oldham, Bury, Tameside and Stockport  
Associate Medical Directors Rochdale, Oldham, Bury and Tameside  
Rochelle Hunt, Head of IM&T  
Julia Wright, Head of HR  
Martin Eastwood, Performance Manager  
Judith Crosby, Senior Management Accountant  
Sarah Corcoran, Risk Advisor  
Tina Shuttleworth, Information Manager  
Louise Burgess, Complaints and Incidents Investigations Manager  
Chris Ryan, Estates Manager

**This document is to be disseminated to all relevant staff, any required discussion or training should be detailed on the return slip.**

**The Policy must be posted on the intranet: Date Posted:**

**The Policy Name, Originator and Review Date should be forwarded to the Risk Management Department for registration: Date Forwarded : 9<sup>th</sup> December 2002**

## Contents

<b>1.</b>	<b>Introduction .....</b>	<b>6</b>
<b>2.</b>	<b>Scope of Security Policy .....</b>	<b>7</b>
<b>3.</b>	<b>Security management .....</b>	<b>7</b>
	Objective: to establish the management structure for information systems security within the Trust.	
3.1	Security management within the Trust .....	7
3.2	National management .....	8
3.3	NHSNet .....	8
3.4	Auditors .....	8
<b>4.</b>	<b>Security Responsibilities .....</b>	<b>8</b>
	Objective: to ensure that all staff are aware of security risks and responsibilities to minimise threats.	
4.1	Management responsibilities .....	8 - 9
4.2	Staff responsibilities .....	9 - 10
4.3	System managers .....	10 - 11
4.4	Local Records Managers/Data Custodians .....	11 - 12
4.5	Information ownership .....	12
4.6	System developers .....	12
<b>5.</b>	<b>Risk management .....</b>	<b>12</b>
	Objective: to identify and counter possible threats to the security of information, communications and systems.	
5.1	Risk management rationale .....	13
5.2	Methodology .....	13
5.3	Reporting .....	14
<b>6.</b>	<b>Security of equipment and information .....</b>	<b>14</b>
	Objective: to protect IM&T equipment and information against loss or damage and avoid interruption to business activity.	
6.1	Equipment siting and protection .....	14
6.2	Equipment maintenance .....	15
6.3	Power supplies .....	15
6.4	Cable routing .....	16
6.5	Remote diagnostic services .....	16
6.6	Security of hard disks .....	16

6.7	Security of equipment off premises .....	16
6.8	Disposal of equipment .....	17
<b>7.</b>	<b>Asset management .....</b>	<b>17</b>
	Objective: to identify and authorise the use of the Trust's IT assets (and to manage capital charges on physical assets).	
<b>8.</b>	<b>Software management .....</b>	<b>18</b>
	Objective: to comply with the law on licensed products; to maintain version control; to minimise the risk of computer viruses; to reduce the risk of misuse of Trust IT equipment; to minimise system malfunction, maintain integrity and avoid disruption of service provision.	
<b>9.</b>	<b>Access control .....</b>	<b>18</b>
	Objective: to minimise the threat of illegal entry to Trust buildings/equipment.	
9.1	Building security .....	18
9.2	Key security .....	19
	9.2.1 External doors .....	19
	9.2.2 Internal doors .....	19
9.3	Keypad access .....	19
9.4	Other keys .....	19
9.5	Identification badges .....	20
<b>10.</b>	<b>Security of third party access .....</b>	<b>20</b>
	Objective: to enable the Trust to control external access to its buildings and systems.	
10.1	Contractors/temporary staff .....	20
10.2	Network security .....	20
10.3	NHSnet requirements .....	21
10.4	Facilities Management (FM) .....	21
<b>11.</b>	<b>User access control .....</b>	<b>21</b>
	Objective: to control user access to systems that are required by their job function.	
11.1	Registering users .....	21
11.2	User password management .....	22
11.3	User passwords .....	22
<b>12.</b>	<b>Information security incident management .....</b>	<b>23</b>
	Objective: to detect, investigate and resolve any suspected/actual information security breach.	

<b>13.</b>	<b>Operational controls and housekeeping .....</b>	<b>24</b>
	Objective: to maintain the integrity and availability of the Trust's Information systems.	
	13.1 Data backup .....	24
	13.2 Media disposal .....	24
	13.3 Virus control .....	25
	13.4 Logging procedures .....	25
<b>14.</b>	<b>Quality control and data validation .....</b>	<b>25</b>
	Objective: to maintain confidence in data accuracy for use in decision-making.	
<b>15.</b>	<b>Systems authorisation, procurement and acceptance .....</b>	<b>26</b>
	Objective: to ensure that all new IT systems are for a defined business purpose and provide an adequate level of security protection. Additionally, they must not adversely affect the security of the existing infrastructure.	
	15.1 Authorisation .....	26
	15.2 Procurement .....	26
	15.3 System acceptance .....	26
<b>16.</b>	<b>Intellectual property rights .....</b>	<b>27</b>
	Objective: to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights e.g. copyright.	
	16.1 Intellectual property .....	27
	16.2 Copyrighted material .....	27
<b>17.</b>	<b>Disaster recovery .....</b>	<b>28</b>
	Objective: to ensure that critical system activities can continue after an unforeseen event leading to a major disruption.	
	17.2 Planning process .....	28
	17.3 Planning framework .....	28
<b>18.</b>	<b>Staff training and awareness .....</b>	<b>29</b>
<b>19.</b>	<b>Key references .....</b>	<b>29</b>

**Appendix A            Legislation and National Policy**

**Appendix B            Assessment Questionnaire**

**Appendix C            Confidentiality Agreement**

## 1. INTRODUCTION

- 1.1 The Trust has a duty to protect its information assets and thus to ensure business continuity and minimise the adverse effects of security incidents. Information assets and the IT systems that support them are becoming increasingly more vulnerable as the potential for wider accessibility is facilitated via more powerful computers and communications networks.
- 1.2 Any loss of the ability to access information could have a significant effect on the efficient operation of the Trust and may result in an inability to provide services to patients and financial loss to the Trust.
- 1.3 Key issues that are addressed by this policy are: -
- **Confidentiality** – access to information is confined to those with specified authority to view the information
  - **Integrity** – information is accurate and kept up to date
  - **Availability** – Information is available to the right person, when it is needed
- 1.4 The Trust also has legal obligations to maintain security and confidentiality of information, notably under The Data Protection Act 1998, Copyright, Designs and Patents Act 1985, Computer Misuse Act 1990 and The Human Rights Act 1998. Additionally, the Trust has to ensure compliance with national policy notably The Caldicott Report, ISO17799 Information Security Management and HSC 1999/053: For the Record (see Appendix A for an explanation of the requirements of legislation and national policy).
- 1.5 The Information Security Policy Manual has been developed to support and enable implementation of the Trust's Information Security Policy.
- 1.6 The Information Security Policy is an official policy of the Trust and as such, sets out the corporate guidelines to be adhered to. It is recognised however, that provision of training for information security within the boroughs of Bury, Rochdale and Oldham currently lies with the Pennine Acute Hospitals NHS Trust under the Service Level Agreements. Training provision for staff within the borough of Tameside and Glossop is available through the Information Security Manager at Pennine Care NHS Trust.
- 1.7 Compliance with Trust policies is a condition of employment and breach of a policy may result in disciplinary action.

## 2. SCOPE

2.1 The Information Security Policy applies to all staff, including temporary staff and students, who record, input, handle, store or otherwise come across information relating to the business of the Trust, its patients/clients and/or its employees.

2.2 Information is defined as:

- Electronic data including facsimiles
- Paper based information
- CCTV and Videos
- Verbal and telephone conversations
- Photographs and other images
- Visually or audio recorded information

2.3 The policy also applies to all Trust IM&T equipment, software and mobile phones whether on or off site.

## 3. SECURITY MANAGEMENT

**Objective: to establish the management structure for information systems security within the Trust.**

### 3.1 Security management within the Trust

The Trust's Head of IM&T is responsible for the implementation and enforcement of the Information Security Policy.

The Trust's Information Security Manager has responsibility for:

- Monitoring and reporting on the state of information security within the Trust
- Ensuring that the Information Security Policy is implemented throughout the Trust
- Developing and enforcing procedures to maintain security
- Ensuring compliance with relevant legislation (see 1.4)
- Ensuring that the Trust's personnel are aware of their responsibilities and accountability for information security through the provision of training/awareness raising
- Monitoring for actual or potential information security breaches

Detailed responsibility for particular systems will be delegated to the relevant systems managers.

The Caldicott Guardian has responsibility for ensuring that all staff conform to the Caldicott principles regarding the protection and use of patient identifiable information.

### 3.2 **National management**

The NHS Executive's Security and Data Protection Programme has responsibility for ensuring that the NHS is able to effectively manage risks associated with the use of computer systems and networks.

### 3.3 **NHSNet**

The process of connection to NHSNet is co-ordinated through the NHS Information Authority.

The Trust is required to adhere to the NHSnet Data Security Policy and sign an associated Code of Connection. This may require the implementation of specific security measures. Such security measures will apply to all systems and users connected to the Trust's Local Area Network (LAN).

### 3.4 **Auditors**

This Information Security Policy manual, its implementation and systems will be subject to periodic review by both internal and external auditors, the recommendations from which will normally be implemented unless specific dispensation is given at Trust management level. Any major security incident could be referred to the auditors for investigation.

## 4. **SECURITY RESPONSIBILITIES**

**Objective: to ensure that all staff are aware of security risks and responsibilities to minimise the threats.**

### 4.1 **Management responsibilities**

Management must:

1. Ensure that all current and future staff are instructed in their responsibilities relating to the security of information.
2. Ensure that all staff using computer systems/media are trained in their use.
3. Ensure that no unauthorised or untrained staff are allowed to access any of the Trust's systems, both computerised and paper based.
4. Written authorisation should be submitted to system managers, for any staff, including temporary staff, requiring access to the Trust's Information systems prior to access being given.

5. Determine which individuals are to be given authority to access specific computer systems. Where the system allows it, the level of access to specific systems should be on a job function need.
6. Implement procedures to minimise the Trust's exposure to fraud/theft/disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas.
7. Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability.
8. Ensure that staff are aware of the need to declare any potential personal conflicts of interest. For instance, an individual working in IM&T procurement should make it known if they or any close relatives have direct interest in a potential supplier.
9. Prior to an employee leaving, or to a change of duties, line managers should ensure that:
  - Passwords are removed or changed as appropriate
  - Relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists
  - Reception staff and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitors pass
  - In rare cases it may be appropriate to assign staff to non-sensitive tasks whilst working out their notice
  - Trust property, including information, is returned. Particular attention should be paid to the return of items that may allow future access. These include personal identification devices, cards, keys, passes, manuals and documents.
9. Where a laptop is shared between users within the department it should be tracked into and out of the department. A record should be kept of its whereabouts and include the date removed, the user, and the date returned to the department.

#### 4.2 **Staff responsibilities**

1. Each Trust employee is **personally responsible** for ensuring that no breaches of information security result from their actions
2. Each Trust employee should declare any potential conflicts of interest (see 3.3 item 7).
3. Each Trust employee must take responsibility for accessing only areas of a system required to fulfil their job function and not access areas within the system, which hold data not relevant to their work.

4. Information is a major asset of the Trust. All staff have a duty and responsibility to the Trust, its patients/clients and to fellow colleagues to protect this asset from unauthorised use, disclosure, access, modification and destruction.
5. Under no circumstances can staff sell or otherwise disclose Trust information for personal profit or gain.
6. Each employee must ensure that the person receiving information is authorised to receive it, where there are doubts checks should be made to ascertain the identity of the recipient prior to disclosure.
7. Employees must report any breaches of security or security incidents to their line manager and/or the Information Security Manager immediately.
8. Wherever possible, sensitive data must be cleared from desks and computer screens blanked when workstations are unmanned.
9. In order to comply with Caldicott guidelines, anyone setting up a database, spreadsheet or manual information system containing patient-identifiable information must first complete an assessment questionnaire (Appendix B).
10. Staff who leave the Trust must ensure that all equipment and information is returned to their line manager prior to leaving.
11. Staff who access computer systems must keep their password secret and never disclose them to colleagues.
12. Any electronic files containing sensitive data must be password protected using the facilities built into the local software.

#### 4.3 **System Managers**

1. Every computer system including e-mail, Internet access and networks will have an identified system manager who will take responsibility for the security of the system and the data therein.
2. Job descriptions for system managers will include specific reference to the security role and responsibility of the post.
3. System managers will ensure that each system has its own detailed 'System Security Policy' that takes into account this policy and national guidelines and is also based on the conclusions of a risk analysis of the particular environment in which the system operates.
4. Access to the Trust's information systems will only be given following written authorisation from the line manager

5. Each system security policy should be reviewed on an annual basis.
6. It is important to ensure that a copy of the documentation outlining the procedures necessary for the secure operations of the system is held securely.
7. All of the Trust's systems should have at least 2 individuals with the expertise to administer the particular system. Where possible, this will include a representative from the IT department and a representative from the department utilising the system.
8. All of the Trust's critical computer systems should have at least 3 individuals with the expertise to manage or administer such a system. Where possible, this will include a representative from the IT department, a representative from the department utilising the system and one other.
9. System managers will be responsible to the Head of IM&T for continued system security.
10. All systems should include validation processes at data input to check in full or in part the acceptability of the data.
11. Systems should report all errors together with a helpful reason for the rejection to facilitate correction.
12. All systems will incorporate internal validation processes and audit trails to detect and record problems with processing/data integrity.
13. The use of 'mandatory fields' should be applied where necessary.
14. Error reports should be produced and actioned regularly.

#### 4.4 **Local Records Managers/Data Custodians**

Local records managers and/or data custodians are essentially system managers (paper and electronic) who have responsibility for:

- Ensuring the system is operated in accordance with this policy
- The information held within their system is secure and used or disclosed in accordance with this policy and/or the Trust's Confidentiality Policy (relating to patient-identifiable information)
- To ensure the accuracy and completeness of the data held within their system. In order to control data integrity, validation checks should be carried out periodically on all data held within the system

- Ensure that output data e.g. printouts etc. are used and disposed of in the appropriate way
- Ensuring that information is kept only for as long as is needed and archived appropriately.

#### 4.5 **Information ownership**

Each set of data will be the responsibility of the system manager, and/or, the data custodian/local records manager and will include:

- Identifying all the data within the area of responsibility
- Agreeing who can access the data, and what types of access each user is allowed
- Determining the classification or sensitivity level of the data
- Periodically reviewing information classifications
- Approving appropriate security controls
- Ensuring compliance with relevant legislation

#### 4.6 **System Developers**

1. The development of new information systems must include consideration of security issues. Any additional costs may be balanced by avoiding a design option which may later have to be abandoned on security grounds, or may need disproportionate effort to make it secure.
2. Anyone setting up a new database or manual information system must inform the Information Security Manager so that the system can be assessed for security in line with this policy.
3. In order to comply with Caldicott guidelines, anyone setting up a database, spreadsheet or manual information system containing patient-identifiable information must first complete an assessment questionnaire (Appendix B).
4. User manuals must be written when new systems are developed in-house.
5. Where possible, systems will incorporate internal validation processes and audit trails to detect and record problems with processing/data integrity.

### 5. **RISK MANAGEMENT**

**Objective: To identify and counter possible threats to the security of information, communications and systems.**

## 5.1 **Risk Management Rationale**

The threats to which information and communication systems can be subjected to continue to evolve, e.g. the introduction of new viruses; at the same time there are new technological developments, such as e-commerce, that bring with them new security issues.

The information infrastructure is not static and it cannot be assumed that a past assessment will provide an accurate reflection of the current state. Each time a security risk assessment is conducted it should examine each information system used by the Trust.

For the Information Security policy to be effective, it must be kept in step with the evolving threats and it will be necessary to periodically validate the applicability of security procedures through conducting a risk assessment.

## 5.2 **Methodology**

All Trust systems will be subject to periodic security reviews by systems managers. The depth of a review will be determined by the importance and size of the particular system.

The risk assessment should be documented, as should any problems that are identified. Action plans should then be developed for removing the weaknesses or introducing system or procedure change.

Reviews should include:

- Identification of assets of the system and their values
- Evaluation of potential threats:
  - The sensitivity of the information being held on each information system
  - The physical security of the accommodation within which information equipment is housed
  - The physical hazards to which the system might be subjected (e.g. fire), including any additional hazards (proximity to danger areas, such as kitchens)
  - The ease with which non-authorised people could get access to information systems
  - The potential for physical tampering (e.g. communication links)
  - The strength of access protection mechanisms (e.g., password protection) and whether users are following security procedures.

- The security of all communication links to the system (e.g. use of encryption)
- If the system audit trails are being logged (e.g. file usage logs)
- Whether users can electronically load data onto the system (e.g. copy files from floppy disks)
- The reliability of data entry protection functions (e.g. Data integrity checks)
- The presence of unauthorised software (e.g. additional copies of a particular application)
- The level of staff turnover and use of temporary staff
  - Assessment of likelihood of threats occurring, including the temptation towards fraud, which the particular system could offer and the extent to which professional hackers might wish to gain access
  - Assessment of the impact of an incident
  - Assessment of the security risks that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets
  - Identification of practical cost effective counter measures/security

Systems are liable to independent reviews by internal and external auditors.

### 5.3 **Reporting**

Each system review will include a formal report to the Head of IM&T containing the findings and recommendations, who will then ensure that the necessary action is taken.

## 6. **SECURITY OF EQUIPMENT AND INFORMATION**

**Objective: to protect IM&T equipment and information against loss or damage and avoid interruption to business activity.**

### 6.1 **Equipment siting and protection**

All IM&T equipment will always be installed and sited in accordance with the manufacturer's specification. Equipment must always be installed by, or with the permission of, the IT department (this includes the attachment of PCs to the network).

All central servers and data communication equipment will be housed in the Trust's secure computer suite. Where appropriate, environmental controls will be installed to protect central/key equipment. Such controls will trigger alarms if environmental problems occur. In such cases, where equipment is sited in a secure area, only authorised entry will be permitted. Drinking and eating is not allowed in the Trust's computer suite and doors will be protected by key-pad access and kept closed at all times.

All IM&T equipment throughout the Trust will be security marked for identification.

All Pc and terminal screens must be positioned so that any confidential information displayed will not be viewable by unauthorised personnel or the public.

Patient identifiable, confidential or sensitive information should not be placed on privately owned computers, palm pilots, filofaxes, personal diaries etc.

## 6.2 **Equipment Maintenance**

All central processing equipment, including file servers, will be covered by third party maintenance agreements.

All personal computers, laptops and printers procured by the Trust will be maintained under warranty with the initial supplier. Out of warranty equipment will be maintained as far as is possible, by the IT Services department provided it is cost effective to do so (each case will be judged on its merits). If individual services require further third party maintenance for specific equipment they will be required to fund the service from their own individual budget. The IT Services department will advise and arrange this cover with an agreed maintenance supplier.

All third parties providing maintenance services on Trust IT equipment will be required to sign confidentiality agreements.

Records of all faults and changes to a system will be maintained by the IT services department in change/fault control logs.

## 6.3 **Power Supplies**

The Trust has generator backup power to the mains electricity supply.

Critical computer equipment must be fitted with battery back-up to ensure that it does not fail during switchovers between mains and generator. Such battery power must suffice for at least 15 minutes at normal usage. Critical equipment will also utilise power management software, which ensures a safe shutdown in the event of power loss to the suite.

#### 6.4 **Cable routing**

All data cabling between buildings will, where possible, be via underground conduits not accessible to unauthorised people. All external cabling installations must be agreed by the IT Services department and after consultation with the Estates department.

All cabling within buildings will be in conduits if surface mounted otherwise, within the framework of the building, and will be terminated at a patch panel that is located in a secure systems cabinet.

Network points will only be patched in the Local Area Network (LAN) if there is a specific requirement for a piece of networked equipment. This will be the responsibility of the IT services department.

#### 6.5 **Remote Diagnostic Services**

Suppliers of Trust systems expect to have dial up access on request to investigate/fix faults. The Trust will therefore permit controlled dial-up access providing there is a genuine need of access and then only after:

- Each supplier has committed to maintaining confidentiality of data and information and to only using qualified representatives.
- Each request for dial up access has been authorised by approved Trust staff, who will only make the connection when satisfied of the need.
- The supplier has been securely authenticated by the Secure-IT remote access server via pre-allocated password tokens.

#### 6.6 **Security of Hard Disks**

Hard disks on any machine may contain sensitive/confidential data. In order to adhere to the principles outlined in the Caldicott report and the Data Protection Act 1998, removal of such disks off site will be judged on its merits balancing the need versus the risk of breach of confidentiality and then only to approved repairers who have signed confidentiality agreements.

#### 6.7 **Security of equipment off premises**

IM&T equipment will not be taken off site, without formal signed approval, other than to transport it from one of the Trust's sites to another.

Laptops/handhelds are vulnerable to theft, loss or unauthorised access and therefore users must ensure they demonstrate good security practices when taking them off site. Laptops that are shared by users within a department should be tracked in and out of the department so

that a record is kept of its whereabouts. In addition, all Trust laptops will be protected with a power-on password to prevent unauthorised access.

Patient and staff information should only ever be processed via a Pc connected to the Trust network, and therefore saved to the Trust network drives. If, however, this is not possible and patient or staff identifiable information is processed via a Trust laptop then the user must contact the Information Security Manager to ensure the appropriate security measures are in place and that the processing of the information in this way is justified in accordance with the requirements of the Data Protection Act 1998 and the Caldicott Report (see Appendix A for an explanation of the requirements).

## 6.8 **Disposal of Equipment**

All IT hardware/software will be utilised and supported until its 'end of useful life', which is:

- The time at which the hardware/software fails to perform satisfactorily the job for which it was purchased and/or
- The job required of the hardware/software has changed and it is not possible to upgrade to meet the new requirements whilst maintaining a satisfactory level of performance.

At such time the equipment will be disposed of via the IT department who will ensure that all hard drives are formatted prior to disposal.

Hardware/software which has not reached the end of its useful life, but which is being replaced, will be considered by a member of the IT department for relocation with the appropriate manager as follows:

- Within the service making the original purchase
- Within the department making the original purchase
- In another part of the Trust

Prior to the relocation of the hardware, all personal data will be erased by the original user and other files and software will be removed by the IT department as required.

## 7. **ASSET MANAGEMENT**

**Objective: to identify and authorise the use of the Trust's IT assets (and to manage capital charges on physical assets).**

An up to date inventory of all Trust IT equipment and disposals of physical computer assets will be maintained by the IT department. This will include the value, location, serial number, security mark and user.

The Trust inventory will also include all items of non-IT equipment costing between £1k - £5k and any high-risk items costing less than £1k. Non IT-equipment on the Trust inventory will be maintained within the individual department.

## **8. SOFTWARE MANAGEMENT**

**Objective: to comply with the law on licensed products; to maintain version control; to minimise the risk of computer viruses; to reduce the risk of misuse of Trust equipment; to minimise system malfunction, maintain integrity and avoid disruption of service provision.**

An up to date register of all proprietary software will be maintained to ensure that the Trust is aware of its assets and that licence conditions are followed.

All licences will be purchased via the IT department and software will only be installed following purchase of the relevant licence. Responsibility for installing software on any Trust owned computer lies with the IT department.

## **9. ACCESS CONTROL**

**Objective: to minimise the threat of illegal entry to Trust buildings/equipment.**

### **9.1 Building Security**

All staff should ensure that the following measures are taken with regard to the security of the building: -

1. Before securing the building/office ensure that all areas are vacated (including toilets/rest rooms).
2. Ensure that all lights and electrical appliances are switched off.
3. Never leave the building/office via the fire exit (unless in the case of an emergency).
4. Ensure that all doors, windows etc are locked.
5. Where applicable, ensure that any alarms are activated.
6. Ensure that all defective doors, windows are repaired as quickly as possible and advise both the Estates department and the Security department of any such defects.

## 9.2 **Key Security**

### 9.2.1 **External Doors**

1. All keys to external doors will be held centrally in the Security Control room where they will be accessible 24 hours a day. Keys will only be issued on production of a Pennine Care NHS Trust identification badge. All keys must be signed in and out.
2. No extra copies of keys must be cut without the authorisation of the Security/Estates Manager.

### 9.2.2 **Internal Doors**

1. All keys to internal doors should be clearly marked – tagged by number rather than description.
2. Internal records should be held in a secure location to identify which keys fit which locks.
3. All keys should be securely stored when not in use, with limited access.
4. All lost keys must be reported to the Security/Estates Manager.
5. The cutting of additional internal keys should only take place with written authorisation from the Departmental Manager.

## 9.3 **Keypad Access**

1. Where keypads are used on external doors, the code should be advised to the Security Manager.
2. Codes should only be advised to staff 'who need to know'. Staff must be informed not to disclose the codes to any other person.
3. Where appropriate codes should be changed on a regular basis, preferably every 6 months.
4. Codes must be changed whenever a member of staff leaves the department.

## 9.4 **Other keys**

Keys to padlocks, cupboards, filing cabinets etc. should also be controlled. It is recommended that: -

1. All such keys should be held centrally in a lockable key cupboard and issued only to those personnel who require access.
2. Keys should be clearly tagged/labelled.

3. The practice of permitting staff to take keys home or carry them about their person should be discouraged.
4. The number of duplicate keys should be kept to a minimum and controlled.

#### 9.5 **Identification badges**

1. All staff on commencement of their employment should be issued with a temporary I.D. Pass from the Security department until such time as the official I.D. Badge has been provided.
2. New starters must be in possession of an I.D Badge request form, which must be completed by line managers before the badge is issued.
3. Staff already in possession of a Trust I.D. Badge who require a replacement must complete a request for replacement I.D. Badge form, available from the Security department.
4. I.D. Badges must be worn whilst on duty.

### 10. **SECURITY OF THIRD PARTY ACCESS**

**Objective: To enable the Trust to control external access to its buildings and systems.**

#### 10.1 **Contractors/Temporary Staff**

If Contractors are known to be commencing work on Trust premises, Departmental Managers should contact the Security department, within their own borough, for the correct procedure that needs to be followed, as temporary I.D. badges will need to be issued.

All contractors, agency and temporary staff are subject to the same checks as permanent staff.

Such personnel, given access to sensitive information held on computers or in manual records must sign a confidentiality statement.

#### 10.2 **Network security**

No external agency (NHS or not) will be given access to any of the Trust's networks unless that body has been formally authorised to have access. All non NHS agencies will be required to sign the Trust's Confidentiality Agreement (see Appendix C).

External agencies will only be allowed access to *their* hardware/systems.

The Trust will control all external agencies access to its systems by utilising strong authentication procedures for each approved access requirement.

### 10.3 **NHSnet Requirements**

The process of connection to NHSnet is co-ordinated through NHS Telecommunications branch.

The Trust is required to adhere to the NHSnet Data Security Policy and sign an associated Code of Connection. This may require the implementation of specific security measures. Such security measures will apply to all systems and users connected to the Trust's Local Area Network (LAN).

The Trust will request that third parties providing remote support do so over NHSnet. Where this is not possible, the NHS Telecommunications Branch will be approached for advice prior to allowing access by third parties to a Trust system.

Strong authentication procedures will be utilised for all dial up connections to the Trust's computer systems.

### 10.4 **Facilities Management (FM)**

FM agencies should conform to both Trust and NHS Executive security requirements.

## 11. **USER ACCESS CONTROL**

**Objective: to control user access to systems that are required by their job function.**

### 11.1 **Registering Users**

In order that only the relevant personnel gain access to the systems they require, a formal application will need to be made to the IT department or System Manager, where appropriate, and, in some cases, to the Head of IM&T.

An authorised line manager must countersign each application for access and provide a valid reason for requiring access.

Access privileges shall be modified or removed, as appropriate, when an individual changes job or leaves. A leavers report will be provided to the IT department from the Human Resources department, each month. The IT department will notify the relevant Systems Manager of any leavers, where appropriate.

## 11.2 **User Password Management**

Passwords are provided to permit access to limited levels of information according to the needs of the department and members of staff. Access should be restricted to those staff directly involved with the input and retrieval of information.

The issues to be considered in user access are:

- Restricting access to certain parts of the record
- Restricting access in terms of access to:
  - Named data about individuals
  - Anonymised data about individuals
  - Aggregated data
    - Restricting user access to a particular “view” of the data
    - Defining what a user can do with the data i.e. create, read, delete, update

All passwords will be specific to individuals and must not be disclosed to others.

Temporary staff should be given their own password, which will be deleted when they leave.

Passwords should be changed regularly – all new systems should include password ageing to force users to change their password periodically. This should never exceed six months and the recommended period is 90 days.

Passwords should be changed whenever there is any indication of possible system or password compromise.

No individual will be given access to a Trust system unless training needs have been identified and they have been made aware of their security responsibilities.

Access to all Trust systems will be restricted by a password facility allowing a level of access on a need to know basis, controlled by the Systems Manager.

## 11.3 **User Passwords**

Staff should ensure that passwords are:

- Not written down (unless this can be stored securely)

- Not easy for others to guess. It is not recommended that users create a password from their spouses name, their telephone number, car registration number or any other obvious association to them.

## 12. INFORMATION SECURITY INCIDENT MANAGEMENT

**Objective: to detect, investigate and resolve any suspected/actual information security breach.**

12.1 A security incident is an event, which has or may result in: -

- The disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact e.g.
  - Embarrassment to the NHS
  - Threat to personal safety or privacy
  - Legal obligation or penalty
  - Financial loss
  - Disruption of activities

Types of incidents that should be recorded include:

- Degraded system integrity
- Loss of system availability
- Disclosure of confidential information
- Disruption of activity
- Financial loss
- Legal action
- Unauthorised access to applications
- Computer misuse
- Records related incident
- Theft or loss of records or IM&T equipment

All incidents indicating a suspected or actual security breach should be reported to the immediate line manager and an incident reporting form completed and sent to the Complaints and Incidents Investigations Manager.

All incidents reported in this way will be recorded on the Incident Management System and a monthly report provided to the Information Security Manager.

Incidents requiring immediate action will be notified to the Information Security Manager within 3 working days of the report being made to the Complaints and Incidents Investigations Manager.

The Information Security Manager/Complaints and Incidents Investigations Manager will advise the relevant Departmental Manager of the action required in response to the incident.

Any major security incident could be referred to the auditors for investigation.

### **13. OPERATIONAL CONTROLS AND HOUSEKEEPING**

**Objective: to maintain the integrity and availability of the Trust's Information Systems.**

#### **13.1 Data Backup**

The Trust will carry out appropriate backups of all its information systems on a nightly, weekly or monthly basis depending on the data change frequency of the system. Tape sets will be stored both within the IT department and elsewhere in the Trust in a secure environment and will be rotated on a weekly basis.

All backups will be verified and logs maintained. In addition, random restore procedures will take place in order to validate backups and test disaster recovery plans.

All Pc users are advised to save their files to the network drives to ensure files are backed up each night. Users should also recognise that floppy disks are an increasingly inappropriate backup medium due to low disk capacity.

Where specialist software applications exist on the network, the users manager should contact the IT department to arrange a regular over-the-network nightly backup of the hard drive.

#### **13.2 Media Disposal**

All removable media such as floppy disks, zip drive disks etc should be reformatted before disposal, however if this is not possible the media should be destroyed.

Paper documents containing confidential information should be disposed of appropriately, when no longer required, either by shredding or by placing in a confidential waste bag provided by the Trust.

### 13.3 **Virus Control**

Computer viruses are a deliberate attempt to destroy or damage data on a computer system. They are transmitted in software, which is innocently loaded onto a computer and can lead to complete loss of data on that system. The Trust therefore seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software.

Users should ensure that *all software and data originating from outside the Trust is virus scanned*. This includes data acquired on floppy disk, on CD-ROM, via email or via the Internet. In addition, users should report any viruses detected/suspected on their machines immediately to the IT department.

The Trust will use the following facilities to ensure the risk of infection is minimised:

- Anti-virus software will be installed on all Pc's in the Trust.
- Anti-virus software will be installed on all susceptible file servers

### 13.4 **Logging procedures**

Where possible, systems should prohibit access after a maximum of 3 unsuccessful login attempts.

All incidents where there have been two or three consecutive and unsuccessful attempts to log on, should be recorded. This will provide an audit to enable the identification of malicious log on attempts.

## 14. **QUALITY CONTROL AND DATA VALIDATION**

**Objective: to maintain confidence in data accuracy for use in decision making**

1. Data accuracy is the direct responsibility of the person inputting the data supported by their line manager. Data relates to information held in computerised format and in manual records.
2. Users are to ensure that the Patient Master Index held within systems is fully searched prior to creating a new patient record.
3. Error correction should be done at the source of input as soon as it is detected. Such correction is increasingly important as systems are linked and errors can be transmitted between systems.

4. Any loss or corruption of data should be reported to the relevant system manager immediately and/or the Information Security Manager to ensure incident reporting mechanisms and, where necessary, the application of disaster recovery procedures (dependant on the severity of the problem – see section 17).
5. Where possible, systems will include validation processes at data input to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity.

## 15. SYSTEMS AUTHORISATION, PROCUREMENT AND ACCEPTANCE

**Objective: to ensure that all new IT systems are for a defined business purpose and provide an adequate level of security protection. Additionally, they must not adversely affect the security of the existing infrastructure.**

### 15.1 Authorisation

The Head of IM&T must approve all major new IT systems and services.

Three levels of authorisation are required:

- **Corporate Approval** – Each system should have appropriate user management approval, authorising its purpose and use. Approval should also be obtained from the manager responsible for the system.
- **Technical Approval** - Where necessary, it should be checked that all devices connected to communication networks or maintained by a particular service provider are of an approval device type.
- **Security Approval** – The Information Security Manager should ensure the system and its implementation conforms to the Information Security Policy.

### 15.2 Procurement

The Trust uses the Prince 2 project management method when procuring systems. The procurement process will incorporate the Trust's security requirements in the statement of need. Prospective suppliers must formally commit to meeting or exceeding these requirements.

### 15.3 System Acceptance

No new systems will be connected to the Trust network until the IT department is satisfied that security has been comprehensively addressed.

All newly procured systems will report all errors together with a helpful reason for the rejection to facilitate correction. Error correction must be done at the source of input as soon as it is detected. Such correction is increasingly important as systems are linked and errors can be transmitted between systems.

## 16. INTELLECTUAL PROPERTY RIGHTS

**Objective: to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights or trade marks.**

16.1 Intellectual property rights can be defined as products of creativity; innovation or research and development. Such property can be given legal recognition of ownership as intellectual property rights through:

- Patents - New technical concepts, inventions
- Copyright - Text, graphics, software, data, art, music
- Design Rights - Form and appearance, technical devices and drawings
- Trademarks – Brands, image
- Confidential Information/Know-how – Ideas/information

The Trust recognises that, from time to time, during the normal course of employment, a member of staff may generate intellectual property. Such Intellectual Property could have commercial or other value. Intellectual Property (actually or potentially) arising from the course of duties of a member of staff, belongs to the Trust unless other formal agreements exist.

### 16.2 **Copyrighted material**

Copyright of material produced by Trust employees would normally remain the property of the Trust. However, the Trust usually grants a free licence to the copyright of any work to be published in a recognised scientific, technical, professional or management journal or book to the author. The Trust will not normally take any action to diminish or remove the moral rights of Trust employees in respect of copyright (i.e. the right to be named as author). The Trust will not grant such licence to the copyright of materials created by a member of staff during the course of and related to their employment. This includes (but is not limited to):

- Course or training materials
- Software programmes

- Any designs, specifications or other works, which may be necessary to protect rights in commercially exploitable intellectual property.

## 17. DISASTER RECOVERY

**Objective: to ensure that critical system activities can continue after an unforeseen event leading to a major disruption.**

- 17.1 The Trust recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event through tested disaster recovery plans.

The Trust recognises that IM&T systems are increasingly critical to the healthcare function and that the protracted loss of key systems or user areas could be highly damaging in operational terms.

### 17.2 Planning Process

The main elements of this process will include: -

- Identification of critical computer systems
- Identification and prioritisation of key users and user areas
- Identification of disaster scenarios and what levels of disaster recovery are required
- Identification of areas of greatest vulnerability based on risk assessment
- Mitigation of risks by developing resilience
- Developing, documenting and testing disaster recovery plans
- identifying tasks, agreeing responsibilities and defining priorities

### 17.3 Planning Framework

Disaster recovery plans will cater for different levels of incidents including: -

- Loss of key user area within a building
- Loss of a key building
- Loss of a key part of the computer network
- Loss of processing power

- 17.4 Disaster recovery plans will always include: -

- Emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel)
- Fallback procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan
- Resumption procedures describing the actions to be taken to return to full normal service
- Testing procedures describing how the disaster recovery plan will be tested

## **18. STAFF TRAINING AND AWARENESS**

Staff training and awareness is critical to the successful implementation of this policy and the prevention of incidents. To maintain staff awareness of their responsibilities, it is recommended that:

- Staff should be released from their duties to attend Information Security Training sessions
- New starters should receive induction training covering:
  - A general discussion on confidentiality
  - Security incident reporting
- Information on new issues within the confidentiality field, and any other relevant and up to date information should be circulated to all relevant staff by the Information Security Manager.

## **19. KEY REFERENCES**

- Ensuring Security and Confidentiality in NHS organisations – NHS Executive’s Security and Data Protection Programme
- The Royal Oldham Hospital Information and Security Policy

## **LEGISLATION AND NATIONAL POLICY**

Many issues surrounding information security are governed by legislation and national policy. The most notable are:

### **Legislation**

- Data Protection Act 1998
- Copyright, designs and patents Act 1985
- Computer Misuse Act 1990
- Human Rights Act 1998

### **National Policy**

- The Caldicott Report
- ISO17799:Information Security Management
- HSC 1999/053: For the Record

## **DATA PROTECTION ACT 1998**

Since March 2000 the key legislation governing the protection and use of identifiable person based information has been the Data Protection Act. The Act does not apply to information relating to the deceased.

The Act gives seven rights to individuals in respect of their own personal data held by others, they are:

- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purpose of direct marketing
- Rights in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

## **The Data Protection Act in practice**

The Data Protection Act applies to 'personal data' that is, data about identifiable living individuals. Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

### ***The rules of good information handling - the principles***

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- \_ fairly and lawfully processed;
- \_ processed for limited purposes and not in any manner incompatible with those purposes;
- \_ adequate, relevant and not excessive;
- \_ accurate;
- \_ not kept for longer than is necessary;
- \_ processed in line with the data subject's rights;
- \_ secure;
- \_ not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual.

## **Information sharing**

The First Principle is one of the crucial principles when considering information sharing. If personal data is to be used for purposes, which were not spelled out to the data subject at the time it was collected, then the "fair processing code" has been breached.

For further information see the Trust's Information Sharing Policy.

## **Access to Health Records**

Data subjects now have access rights to all records irrespective of when they were created, although under section 30 access to some health, education and social work data may be constrained or denied. Where there is a joint

personal record, all parties must have arrangements in place to provide access.

The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased. The Access to Health Records Act 1990 provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

For further information see the Trust's Access to Health Records Policy.

### **COPYRIGHT, DESIGNS AND PATENTS ACT 1985**

Under UK Copyright Law, persons involved in the illegal reproduction of software can be subject to unlimited civil damage and to criminal penalties, including fines and imprisonment.

Copyright protects against copying the expression in a work, not against copying the work's idea. When a new work is created by copying an existing copyrighted work, copyright infringement exists if the new work is substantially similar to the work that was copied.

The illegal copying of software is strictly forbidden within the Trust. Employees who make, or use unauthorised copies of computer software will be disciplined as appropriate under the circumstances. This may include termination of employment.

### **COMPUTER MISUSE ACT 1990**

This Act is intended to protect data held on computers from unauthorised access. It creates three new offences:

1. Unauthorised access to computer material;
2. Unauthorised access with intent to commit or facilitate further offences;
3. Unauthorised modification of computer material.

The misuse of computer hardware or software may involve one or more offences being committed. For example, a person who falsifies the data in an account held on a computer by inputting false information can be convicted of falsification of accounts, contrary to the Theft Act 1968, S17, if he acts with a view to gain or intent to cause loss.

The Council of Europe has developed a series of proposals relating to computer related crime. The Computer Misuse Act 1990 provides a balance between the requirements of a data user to protect personal information and the sanctions against someone who attempts to gain unauthorised access. However, information systems security measures cannot rely entirely on

individuals being deterred from gaining unauthorised access to data by the possibility of prosecution.

## **HUMAN RIGHTS ACT 1998**

Article 8.1 of the Human Rights Act provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This is however a qualified right, i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and article 8.2 provides “there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

## **THE CALDICOTT REPORT**

This report, undertaken by Dame Fiona Caldicott, was published in December 1997 giving 16 recommendations on the **non-clinical** use of patient-identifiable information in the NHS. While generally supporting the purposes for which patient information is currently used, the report called for improvements to be made in the way such information is handled.

Patient-identifiable information is personal information that can be traced back to a living individual. In some cases a post code or NHS number may be sufficient to trace an individual.

Two major concerns arising from a review between December 1996 and June 1997 were:

- A variable awareness throughout the NHS of confidentiality requirements outside the clinical setting.
- A need to ensure that information which can readily identify individual patients is kept to a minimum.

The Caldicott report mandated action to meet the following recommendations:

1. Every dataflow, current or proposed, should be tested against basic principles of good practice. Continuing flows should be re-tested regularly.
2. A programme of work should be established to reinforce awareness of confidentiality and information security requirements amongst all staff within the NHS.
3. A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.

4. Clear guidance should be provided for those individuals/bodies responsible for approving uses of patient identifiable information.
5. Protocols should be developed to protect the exchange of patient identifiable information between NHS and non-NHS bodies.
6. The identity of those responsible for monitoring the sharing and transfer of information within agreed local protocols should be clearly communicated.
7. An accreditation system, which recognises those organisations following good practice with respect to confidentiality, should be considered.
8. The NHS number should replace other identifiers wherever practicable, taking account of the consequences of errors and particular requirements for other specific identifiers.
9. Strict protocols should define who is authorised to gain access to patient identity where the NHS number or other coded identifier is used.
10. Where particularly sensitive information is transferred, privacy enhancing technologies, i.e., encryption must be explored.
11. Those involved in developing health information systems should ensure that best principles are incorporated during the design stage.
12. Where practicable, the internal structure and administration of databases holding patient identifiable information should reflect the principles developed in the Caldicott report.
13. The NHS number should replace the patient's name on Items of Service claims made by General Practitioners as soon as practically possible.
14. The design of new systems for the transfer of prescription data should incorporate the principles developed in the Caldicott report.
15. Future negotiations on pay and conditions for General Practitioners should, where possible, avoid systems of payment, which require patient identifying details to be transmitted.
16. Consideration should be given to procedures for General Practice claims and payments, which do not require patient identifying information to be transferred, which can then be piloted.

From the recommendations came six good practice principles:

- **F**ormal justification of purpose.
- **I**nformation transferred only when absolutely necessary.
- **O**nly the minimum required.
- **N**eed to know access controls.

- All to understand their responsibilities.
- Comply with and understand the law.

## **BS7799: INFORMATION SECURITY MANAGEMENT**

The standard is published in two parts;

- BS 7799-1: 1999 - Code of practice for information security management
- BS 7799-2: 1999 - Specification for information security management systems

Part 1 is an introduction to the practice of Information Security and describes the key controls necessary to ensure an effective security implementation.

Part 2 specifies the requirements for establishing, implementing and documenting an information security management system (ISMS) and forms the basis for an assessment of the ISMS. The standard requires a risk assessment and the identification of the most appropriate control objectives. A set of detailed controls is then described which can be used to achieve the control objectives as applicable. These controls are:

- Security policy
- Security organisation
- Assets classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- System Access control
- System development and maintenance
- Business continuity management
- Compliance

## **HSC 1999/053: FOR THE RECORD**

This circular, from the Department of Health, required all NHS organisations to develop a records management strategy to ensure that records of all types (administrative as well as medical) are: -

- properly controlled
- readily accessible and available for use, and eventually
- archived or otherwise disposed of

The strategy should ensure that information was available:

- to support patient care and continuity of care
- to support day-to-day business, which underpins delivery of care

- to support evidence based practice
- to support sound administrative and managerial decision making, as part of the knowledge base for NHS services
- to meet legal requirements, including requests from patients under access to health records legislation
- to assist medical and other audits
- to support improvements in clinical effectiveness through research and also support archival functions by taking account of the historical importance of material and the future needs of research
- whenever, and wherever there is a justified need for information, and in whatever media it is required.



**ASSESSMENT QUESTIONNAIRE  
FOR THE DEVELOPMENT OF SYSTEMS CONTAINING  
PATIENT IDENTIFIABLE INFORMATION**



4. Do you intend to store these data on a computerised system?

Yes  No

*If you answered No please go to question 7.*

5. Do you intend to use skills from within your department to develop and support a software application for managing this dataset?

Yes  No

*If you answered No to question 5, please go to question 6, otherwise please go to question 7.*

6. Have you identified funding from your own budget to commission an external supplier to develop the software application on your behalf?

Yes  No

7. Please state the benefits (e.g. to the patient/client/clinician) of collecting this dataset.


8. Please state any risks associated with not collecting this dataset.


*Completed by:*

*Name:* ..... *Workplace:* .....

*Job Title:* .....

*Telephone No:*

*Date:*

.....

*Return to: Caldicott Guardian  
Pennine Care NHS Trust Headquarters  
Tameside Hospital*

*Copy to: Information Manager  
Tameside Hospital*

## **Confidentiality Agreement**

Actions:

1. Send two copies of the agreement to the third party for signature
2. On return, send both copies to the Caldicott Guardian for signature
3. The department head will sign both copies, send one to the third party for their records, keep one copy, which should be photocopied and sent to the Information Security Manager so that a central register of all agreements can be kept.

## Confidentiality Agreement

### 1. Introduction

The Data Protection Act and other legislation relating to information security bring a number of changes and, in particular, impose certain obligations on users of information. It is important that adequate security measures are in place to ensure that the information is only used for the purpose for which it has been provided and that there is no unlawful disclosure or loss of the same.

For the Trust's compliance with legislation, the Trust has developed this confidentiality agreement. A party (hereinafter called "the Requestor") must sign and comply with this Agreement in order to obtain access to personal information held by the Trust.

**This Agreement should only be used where there is no existing contract between the parties that already adequately deals with the matter of personal information confidentiality.**

This Agreement shall come into effect on the last of the dates below the signatories of the Trust and the Requestor. However it may apply retrospectively to any relationship between these parties if a date is included hereafter:

**This Agreement shall apply retrospectively from the date of**

.....**200** [delete if not applicable]

### 2. Information sharing

- 2.1 The Requestor may request certain personal information relating to individuals and other information (images, research, finance). However, the use of information must be in accordance with the terms of this agreement.

### 3. Code of confidentiality

The Requestor undertakes that it:

- 3.1 Shall maintain the information received in strict confidence and shall not forward the information or a copy of it, in whole or in part, to a third party except in the case where it is necessary for the Requestor to perform any obligation(s) owed to the Trust or which arise under statute **and where the third party:**

- (a) is or will be contracted to the Requestor; and
  - (b) requires the said information in order to perform the said contract;  
and
  - (c) has first signed a copy of this Confidentiality Agreement direct with the Trust.
- 3.2 Shall not make use of or otherwise process the information other than for the strict purposes as agreed with the Trust.
- 3.3 Shall restrict access to the information solely to its responsible employees and/or the aforesaid third party's employees who need to have such access to it for the purposes agreed with the Trust.
- 3.4 Acknowledge the Trust's and patients' legal rights in the information received and that the disclosure to a third party of any information shall not confer upon the third party any rights whatsoever in respect of any part of such information, **except for the purposes expressly agreed as between the third party and the Trust.**
- 3.5 Shall take only those copies of any document or other material necessary for the purposes as agreed with the Trust. The Requestor shall immediately on request by the Trust return any information together with any copies or extracts taken by the Requestor. The Requestor shall write to the Trust to confirm that the Requestor has carried out the Trust's request and has fully complied with this agreement.

#### **4. Information security undertaking**

The Requestor hereby undertakes the following:

- 4.1 Where processing personal or sensitive information, the Requestor must comply in all respects with the provisions of the Data Protection Act 1998 and other relevant legislation (including any amendment or re-enactment thereof).
- 4.2 Shall fully indemnify the Trust against any claims arising at common law and/or

- (a) under the Data Protection Act; and/or
- (b) under other relevant legislation

as a result of a breach of the terms of this agreement.

- 4.3 Notify the Trust immediately of any notice or notification served on, or sent to, the Requestor Commissioner under the Data Protection Act. This particularly includes any de-registration, enforcement or transfer prohibition notice.

- 4.4 Notify the Trust immediately of any notice served on the Requestor regarding an individual in connection with any unauthorised disclosure of personal information.
- 4.5 Comply in all respects with the provisions of the Computer Misuse Act 1990 and Copyright Designs and Patents Act 1988 and of any other relevant legislation (including any amendments and/or re-enactment thereof).
- 4.6 Restrict access to personal information solely to responsible employees who need to have such access to it for the purpose of processing personal information and who have undertaken training in the use of personal information to a standard reasonably required by the Trust.
- 4.7 Not assign or sub-contract the whole or part of the processing of information to a third party without the prior written consent of the Trust.
- 4.8 Should the Trust agree to another party/sub-contractor (pursuant to clause 4.7), then that other party must first sign a copy of this Agreement as between it and the Trust, before carrying out any processing.
- 4.9 Allow the Trust on reasonable notice to inspect any premises where the processing of information takes place and for the Trust to inspect and copy any relevant documentation in order for the Trust to satisfy itself that the Requestor is complying with the provisions of this agreement.
- 4.10 Use best endeavours to immediately destroy or order the destruction of the information in the Requestor's control or possession, or at the Trust's request to return said information, (including any copies of the information on any media whatsoever), on completion of its use for the agreed purpose(s).
- 4.11 On destroying or returning the information the Requestor shall inform the Trust accordingly and the Requestor shall thereby warrant that the Requestor has acted accordingly.

## **5. Breach of confidentiality**

The Requestor undertakes that:

- 5.1 Should a breach of this agreement occur by a member of the Requestor's staff, the Requestor shall immediately inform the Trust of the incident.

**6. Jurisdiction and Applicable Law**

6. The parties hereby accept the exclusive jurisdiction of the English courts and agree that the contract is to be governed and construed according to English law.

**Instructions for execution of this Agreement:**

Please indicate your acceptance of the above by signing this agreement in duplicate and returning both copies to the Trust. **Do not sign this Agreement unless you intend to be legally bound by its contents and obligations.**

**The parties' authorised signatories must initial the left margin at clause 1, retrospective date, if this clause has been deleted.**

**For and on behalf of the Trust:**

Authorised Signatory:  
(Caldicott Guardian)

Name:

Title:

Date:

Authorised Signatory:  
(Department Head)

Name:

Title:

Date

I/We agree to the terms contained in this agreement:

The Requestor's name:

Authorised Signatory:

Title:

Date:

