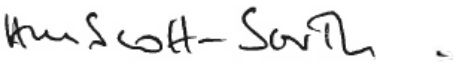
Burton Hospitals

NHS Foundation Trust

INFORMATION SECURITY POLICY

POLICY DOCUMENT

Approved by:	**Trust Executive Committee**
On:	**29 March 2017**
Review Date:	**May 2019**
Corporate / Directorate:	**Corporate**
Clinical / Non Clinical:	**Non Clinical**
Department Responsible for Review:	**Information Department**
Distribution:	
• Essential Reading for: • Information for:	All staff including bank staff and volunteers, non Trust employees, S&S Health Informatics Service (HIS) staff, ICT suppliers and partners
Policy Number:	**6**
Version Number:	**7**
Signature:	
	Chief Executive
Date:	30 March 2017

Burton Hospitals NHS Foundation Trust

POLICY INDEX SHEET

Title:	**Information Security Policy**
Original Issue Date:	**1996**
Date of Last Review:	**February 2017**
Reason for amendment:	**Periodic review**
Responsibility:	**Head of Business Intelligence**
Stored:	**Information Department home drive\Information Governance\Information Security folder**
Linked Trust Policies:	**Information Governance Policy Confidentiality Policy User Access Management Policy Records Management Policy Condemned Equipment - Disposal of Surplus - Obsolete - Condemned Equipment Employee Use Of Social Media And Social Networking Policy**
E & D Impact assessed:	**EIA 159**

Consulted:	**Information Governance Steering Group, S&S Health Informatics Service (HIS) Executive Directors and Line Managers**

REVIEW AND AMENDMENT LOG

Version	Type of change	Date	Description of Change
3	Review	19/12/2011	Periodic review and update of Version 3
4	Review	23/01/2012	Periodic review and update of Version 4
5	Review	23/12/2013	Amendments regarding use of personal equipment, access to social media sites and general review
6	Review	17/11/2015	Periodic review and update of Version 5
7	Review	20/02/2017	Periodic review and update of Version 6

INFORMATION SECURITY POLICY

CONTENTS

BURTON HOSPITALS NHS FOUNDATION TRUST

INFORMATION SECURITY POLICY

1. INTRODUCTION

Information held within the Burton Hospitals NHS Foundation Trust' s (the Trust's) manual and computer systems represents a valuable corporate resource on which the organisation is highly dependent for carrying out its day to day activities. Disruption to these systems potentially has a great impact on the ability of the Trust to treat patients. The three main issues are:

Confidentiality	Information is only accessed by those who "need to know"
Integrity	Data are valid, complete and fit for purpose
Availability	The correct information is accessible to the person who needs it at the right time.

Due to the rapidly changing nature of Information Technology this Policy will be amended as new threats to security arise.

2. POLICY STATEMENT

The purpose of this Policy is to protect information from misuse and to ensure it is available to support the organisation in delivering healthcare. In particular the Trust will ensure that:

- Measures are put in place to manage risks to Cyber-Security
- Data held on its computer systems are secure and confidential
- Transfers of data are carried out securely
- The Data Protection Act and other relevant legislation are complied with
- NHS guidance in this area including the Information Governance framework requirements are implemented
- Confidentiality, integrity and availability of data are maintained at all times
- There are systems for reviewing, monitoring, and improving security
- Joint working with partner organisations maintains and improves security
- Employees are made aware of this Policy and its implications

Failure to comply with this Policy may be dealt with under the Trust's disciplinary procedures.

3. COVERAGE AND SCOPE

This Policy applies to all Trust employees whether working on or off site and other users of the Trust's information systems including Non-Trust Employees (NTEs) and Contractors.

In addition the Policy is applicable to all Trust owned computer systems, externally provided systems where the Trust has local responsibilities, and employee owned devices authorised for use on Trust business.

4. DUTIES AND RESPONSIBILITIES

Security must be the responsibility of all employees in the organisation rather than being confined to a few specialists. The specific duties at each level are detailed below.

The Executive Director with responsibility for Information Security is the Director of Finance, Performance, Information and Estates, who is also the Trust's designated Senior Information Risk Owner (SIRO). Day to day management responsibility for Information Security is delegated to the Head of Business Intelligence.

The SIRO will ensure that the Board of Directors is briefed on Information Security issues, develop an Information Risk Management Programme and provide an annual risk assessment for the Annual Governance Statement .

The Head of Business Intelligence is the designated Trust officer for Information Security and Data Protection and will support the SIRO and other key Trust staff e.g. the Caldicott Office Function in such matters. They will also be responsible for the implementation of the Information Risk Management Programme.

The Chief Information Officer (CIO) or Caldicott Office Function will chair the Information Governance Steering Group which is charged with overseeing the Information Security arrangements in the Trust including the review and implementation of this Policy.

The IT Operations Manager will be responsible for approving applications for mobile computing and remote access. They will keep records of approvals and a list of equipment issued.

Departmental managers are responsible for ensuring that all staff have been properly trained to use computer systems and that this Policy is complied with. In addition it is essential that they promptly notify Human Resources of new starters and leavers.

Information Asset Owners and Administrators have a key role in ensuring security and confidentiality and should note their particular responsibilities - see section

6.5 Information Asset Owners and Administrators . Where a departmental system does not have a designated Information Asset Owner then this role will be assumed to be the responsibility of the Head of Department.

All employees have a personal responsibility to comply with this Policy; **failure to do so may be dealt with under the Trust's disciplinary procedure.**

5. COMPUTER SECURITY POLICY

5.1 Cyber–Security

The Trust's Information Technology (IT) infrastructure is essential to the smooth running of daily business processes and the delivery of healthcare. This infrastructure is subject to potential Cyber-Security threats such as hacking, virus attack, and data leakage. These threats can be countered by good Information Security in general; however the following specific measures have been implemented:

- Timely response to threat alert (CareCERT) Bulletins issued by NHS Digital
- Penetration Tests of the Trust's IT infrastructure
- Vulnerability scans of internal servers

The adequacy of these measures will be kept under review and strengthened where required.

5.2 Individual Passwords

Access to Trust computer systems is protected by password. These may be system generated (e.g. Meditech) or chosen by the user. If the latter, the password must be at least 8 characters long and a mix of upper and lower case characters including special characters. The chosen password must not be something that can be easily associated with the user.

Passwords must not be disclosed to any other person and should not be written down or displayed on or near computer equipment. Do not write any passwords down unless concealed, disguised, or encrypted.

The use of another person's password is forbidden. If you think your password has become known by another person, notify your Line Manager and get it changed immediately.

The Microsoft Windows screensaver must be password enabled. The timing frequency should be appropriate to the risk - i.e. a maximum of five minutes. If you require assistance please contact the S&S Health Informatics Service Desk (HIS) via the HIS Service Desk Portal on the Trust's Intranet homepage.

It is essential that password access is removed from staff who leave the Trust; please ensure that the correct procedure is followed (See ESR Manager Self Service Manual on the Human Resources Intranet site under the section Central Staffing – including Payroll, Expenses and ESR queries).

5.3 Misuse of Computer Resources

The use of the Trust's computer equipment for purposes not connected with the work of the Trust is not allowed. Only persons authorised by Management may use the Trust's computer equipment.

The storing of personal files on Trust equipment, e.g. images, music files etc is not permitted. Reports can be run by the S&S HIS to identify those members of staff storing high volumes of data who will be contacted to discuss the content and removal.

Deliberate unauthorised access to, copying of, alteration or deletion of programs and data will be regarded as a breach of this Policy and may be dealt with under the Trust's disciplinary procedures.

5.4 Reporting of Security Incidents

It is essential that all suspected or actual breaches of computer security are reported **promptly**.

A breach of computer security is defined as any action or incident which has caused, or could result in, the willful or accidental unauthorised access, disclosure, alteration, corruption or deletion of any data held on or produced by a computer which relates to a patient, a member of staff or the commercial activities of the Trust and its purchasers and suppliers. Examples of security incidents include:

- The disclosure or loss of confidential information
- Your password becoming known to someone else
- Virus infection of a computer or media e.g. CD or DVD
- Cyber-related incidents .e.g. Denial of Service (DoS) attacks, Phishing emails, Social Media disclosures and Spoof websites
- Unauthorised access to or use of information
- Viewing your own clinical or staff record

*Disclosures involving manual patient records e.g. case notes should be reported to the Health Records Manager on Ext. 5466 as well as your Line Manager (See "Unauthorised Disclosure of Manual Records").

A security breach leaves both the Trust and individual liable to prosecution under the Data Protection Act and Computer Misuse Act.

The incident should be reported to your Line Manager and the HIS Service Desk via the S&S HIS Service Desk Portal on the Trust's Intranet homepage. In cases where it is your Line Manager that is suspected then report it to the manager above.

The incident will be investigated by the HIS Governance Lead who will keep Trust personnel appropriately informed. There is an escalation procedure to involve more senior staff in serious cases. A log of incidents is kept by the S&S HIS on behalf of the Trust. This is reviewed periodically to establish whether security measures need to be improved.

All staff are individually responsible for reporting security incidents.

NB Incidents also need to be recorded on the Trust's Datix Incident Reporting system.

5.5 Physical Security

All employees should ensure that the following security measures are applied and observed within their respective Wards and Departments etc.

PCs should be sited as to avoid the possibility of confidential information being seen by unauthorised persons.

PCs should be logged-off when left unattended. This will ensure that confidentiality and access controls are properly maintained. Failure to log-off from systems when unattended may provide other users with additional computing facilities than would normally be allowed.

Where PCs are provided with security devices (e.g. security locks etc), these should be used to secure the equipment from unauthorised use or theft.

Mobile devices e.g. Laptops, Tablets etc must be securely locked away when not in constant use (e.g. overnight, at weekends etc).

Trust provided encrypted memory sticks must be used to store Trust data, the use of personally owned memory sticks is forbidden. Trust owned memory sticks must be kept securely at all times.

5.6 Computer Printout

Carefully consider whether you need a hard copy of the information before printing out. Reducing printed material will lower the chances of confidentiality breaches.

Computer printout shall only be released to authorised staff.

Output shall not be retained for longer than it is required, but should be retained for the minimum period as defined by law.

Waste printout must be disposed of with due regard to the sensitivity of the information it contains. Confidential information must be disposed of securely, e.g. via the "Shred-it" consoles or by shredding. Confidential waste skips must not be used.

5.7 Mobile Computing and Remote Access

Due to the nature of their role some Trust staff need mobile computing equipment and/or the requirement to connect to Trust computing facilities from remote locations. This has increased security risks and special arrangements need to be in put in place. These apply to users of Laptops, iPads, tablets, Smart Phones, and any user connecting by remote access.

The Trust will provide secure access to email/calendar/contact data for Trust staff from personal portable devices, such as Smartphones, iPads, and tablets. Access must be individually applied for and authorised. The connection of non-authorised personal devices to the Trust's computing facilities is forbidden.

All applications for mobile and remote access services must be made to the IT Operations Manager. Please email AllysonJones@burtonft.nhs.uk

Users must comply with the Mobile Computing and Remote Access Procedures which are issued to them as part of the application process.

The user should treat the remote connection with the same consideration that would be given to an on-site PC. Remote connection must only be made via a Trust authorised device.

The Information Security Policy must be complied with when using remote services or mobile equipment.

Patient/person identifiable data must not be saved or downloaded to the remote/mobile device hard disk or other media e.g. CD, Encrypted Memory Stick, or printed out.

Concurrent connection to the Trust network and any other network e.g. the Internet is not permitted.

5.8 Assessment of New Systems

It is essential that all new systems are assessed for compliance with Data Protection and Information Security standards. This applies to any computer system including those provided free of charge e.g. as part of a national initiative. It also includes remote systems accessed via Internet web links. The assessment usually takes place as part of the implementation process but if you think it has been missed please contact the Information Governance Officer Helen.Alty@burtonft.nhs.uk via email or on Ext. 2031.

5.9 Internet User Policy

Whilst the Internet enables rapid communication and access to information it also exposes the Trust to greatly increased security risks. These include unauthorised access to information, virus attack, and hacking.

The Trust has secure access to the Internet via the NHSnet gateway for accessing information and for email (see also Email User Policy). Connection to the main Trust network and the Internet (other than via NHSnet) at the same time is forbidden.

During normal working hours Internet access is permitted only for a work related purpose. However personal access via NHSnet is permitted before or after work, or during lunch breaks. The downloading of multimedia and MP3 files for personal use is not permitted.

The accessing of material of an inappropriate nature is forbidden. This

includes but is not limited to material that is indecent, obscene, sexist, racist, or pornographic, or which may cause offence. In addition, use must not contravene the Computer Misuse Act 1990, specifically, hacking is not permitted.

Please note that use of social media sites e.g. Twitter, Facebook etc. is governed by the Employee Use of Social Media and Social Networking Policy.

Users must ensure that the use of information obtained via the Internet complies with copyright law.

Internet usage is monitored centrally by individual user in order to protect the Trust's computing resources and to ensure compliance with legislation and NHS policy.

Confidential information must not be passed via the Internet.

Internet usage is subject to ongoing review and further restrictions may be imposed to protect the Trust's computing resources, reputation, or to comply with NHS mandate or legislation.

Failure to comply with this Policy may be dealt with under the Trust's disciplinary procedures.

5.10 Email User Policy

In order to perform their duties Trust staff are given access to email via a centrally managed service. Along with the benefits this brings it is recognised that there are increased security risks.

Sharing Information Securely

Confidential information regarding patients and staff must not be sent externally via email unless encrypted. The NHSmail email service is the only secure method for external email as messages and attachments are automatically encrypted. However it is essential that both the sending and receiving accounts are of this type. To request an NHSmail account please contact the S & S Health Informatics Service Desk (HIS) via the HIS Service Desk Portal on the Trust Intranet homepage.

Within the NHSmail

Emails sent within NHSmail, i.e. between two @nhs.net accounts – are always sent securely. Emails are also sent securely between @nhs.net and @hscic.gov.uk

Within Government

Email is passed between the following email domains and @nhs.net securely:

Department	Domains
Central Government	*.gsi.gov.uk *.gse.gov.uk *.gsx.gov.uk Note that @orgname.gov.uk is not secure
Police and Criminal Justice	*.pnn.police.uk *.scn.gov.uk *.cjsm.net
Local Government	*.gcsx.gov.uk
Defence	*.mod.uk

Within other areas

Emails sent to other email systems (including NHS.uk) are not transmitted securely. Personal or sensitive information must therefore be encrypted. NHSmail provides an encryption tool which enables information to be shared securely.

Users must be aware at all times that email is frequently used to attempt to gain unauthorised access to systems (hacking) or to commit fraud. Do not open email attachments or click on links in emails unless you are sure they are genuine. Do not reveal your passwords in response to email requests or personal details such as bank account information. If you are concerned about an email you have received please contact the S&S HIS Service Desk via the Portal immediately.

Care needs to be taken when addressing messages as it is easy when using distribution groups to circulate an email more widely than intended.

The sending of inappropriate material by email is forbidden. This includes but is not limited to material that is indecent, obscene, sexist, racist, or pornographic.

Email usage must comply with the Data Protection Act - please see section 6 of the Information Security Policy.

Users need to note that statements made in emails must be factual and truthful and do not contain, for example, inaccurate gossip. Where incorrect statements are made about individuals and companies, the Trust is potentially liable.

Users must ensure that information circulated via email complies with copyright law.

The use of Web based email e.g. "Hotmail" is not permitted for work related purposes.

Copies of emails sent by the Trust central service are stored on the email server for backup purposes.

The sending of email for personal rather than business use is not permitted.

The use of the service will be monitored by individual user to ensure compliance with this Policy. Email access may be removed from anyone abusing it. Should the Trust incur charges due to inappropriate use these will be recharged to the individual user.

The above applies equally to all electronic messaging systems used by Trust personnel.

Auto forwarding

Users should not automatically forward their email to a commercial ISP (Internet Service Provider) i.e. Hotmail to enable access at home.

Users sending email must be aware that it is not suited for confidential communications. Various systems are used for receiving email and there is not guarantee that the addressee will be the only person to see the mail.

5.11 Computer Viruses

Viruses are usually spread via email or the Internet but can also be carried on USB memory sticks or CDs being passed around users of different PCs. Computer games and "demonstration" CDs are also a possible source of infection. **A PC is usually infected by opening a virus infected file within an email, memory stick or on a CD.** The Trust has software installed on its computer systems which regularly check for viruses.

In order to reduce the risk of virus infection the following should be observed.

Please note that it is becoming ever more difficult to identify “phishing emails” as they become more sophisticated and they appear to look genuine, however the tell-tale signs are usually:

- They are sent by an unrecognised sender – although in some cases they can appear to be from someone you know
- They relate to something that is usually out of the ordinary e.g. HMRC contacting you about a tax return on your work email, or receiving an invoice for payment when this is not part of your job role
- The sender will use poor grammar or the e-mail will contain spelling mistakes
- Take care when opening e-mail with attachments. Check that you know who the sender is and that the subject/title is meaningful. Even if you know the sender it may still carry a virus

Never respond to such emails and never click on any embedded link or open the attachment. Such actions can have huge consequences for the Trust and impact on computer services. If in doubt do not open the email and contact the S&S HIS Service Desk via the portal.

All "incoming" CDs, including disks from other NHS Organisations, demonstration disks and new software packages should be checked for viruses before they are used. Please contact the S&S Health Informatics Service Desk (HIS) via the HIS Service Desk Portal on the Trust's Intranet homepage.

The introduction of unauthorised Computer software will be considered as misuse of the Trust's Computer resources and may be dealt with under the Trust's disciplinary procedures.

It is essential that the anti-virus software is updated *regularly* so that the latest viruses can be detected. This should be done automatically via the network. *If you suspect that your software has not been updated then please contact the S&S Health Informatics Service Desk (HIS) via the HIS Service Desk Portal on the Trust's Intranet homepage*.

If you detect a virus you MUST report it to the HIS Service Desk via the HIS Service Desk Portal on the Trust's Intranet homepage.

They will be able to advise on what action to take and will record the incident in the Computer Security Log.

5.12 Backing up data

Your data must be regularly backed up. Data stored on the network servers will be automatically backed up by the S&S HIS each night. Trust PCs are set up to save data by default on a network drive rather than the "C" drive. If you suspect this is not the case or there are other problems please contact the S & S HIS Service Desk via the S&S HIS Service Desk Portal on the Trust's Intranet homepage.

It is the individual user's responsibility to ensure that data are backed up by saving it on a network drive.

It is no longer necessary to back up your own data but any historical files must be kept securely and disposed of safely when no longer required.

When working on spreadsheets, documents etc. ensure that you save the files at regular intervals.

5.13 Portable Computers

Portable Computers (e.g. Laptops and Notebook PCs) are increasing in use by Trust employees especially where there is a requirement to work at more than one location e.g. office and home. For these users there are some specific security measures that need to be complied with as follows.

- The equipment must be encrypted
- It is only to be taken off site if authorised by your Line Manager
- You are responsible for the equipment whilst it is in your possession

- The equipment must be kept securely when not in use
- Do not leave it on view e.g. in a car, or near ground floor windows
- Use any security measures provided e.g. locking cables
- Back up any data kept on the hard disk to a network drive

It is essential that any security problems e.g. loss, theft, virus infection, are reported promptly. See "Reporting Security Incidents". Users connected to the Trust network from off site also need to comply with the "Remote Access" section of this Policy and the Mobile Computing and Remote Access Procedures.

5.14 Security

Lock away any computer equipment where practical.

Use security locks if provided.

Equipment should not be removed from the Trust's premises without prior approval.

Personal data should not be left displayed on the screen when the PC is left unattended (i.e. always log out).

Keep CD's, DVD's and encrypted memory sticks etc. locked away when not in use.

Always log off when you have finished your session on the PC. This will ensure that other users do not gain access to any facilities or files available only to yourself.

5.15 Buying Hardware and Software

All purchases of Hardware and Software have to be approved centrally. This is to ensure:

- It is suitable for its intended purpose
- Compliance with Trust and NHS Standards
- Where possible Hardware/Software is standardised
- Compatibility with the Trust's Information Strategy

It is Trust policy to buy DELL PCs in all but exceptional circumstances.

To order new equipment please contact the S & S HIS Service Desk via the HIS Service Desk Portal on the Trust's Intranet homepage.

NB Procurement are instructed not to order computer equipment unless authorised.

5.16 Transfer of Computer Equipment within the Trust

Users are not authorised to move fixed equipment, e.g. PCs and printers. Please ensure that the following are carried out when transferring equipment:

- Inform the S&S HIS Service Desk via the HIS Service Desk Portal on the Trust's Intranet homepage that the equipment is to be moved. A S&S HIS engineer will attend the new location where the transferred equipment is to be installed. The S&S HIS will update the Trust's Asset Register.

- No data should be stored on the PC Hard Disk; however if any data needs to be removed the HIS engineer will advise the user of the process to be followed.

- If software is to be transferred with the PC then the relevant licence, program CDs and manuals should be also passed on.

- If the software licence is to be retained then the program should be removed from the Hard Disk before transfer.

If the equipment is to be permanently disposed of please see "Disposal of PCs" section below.

The S&S HIS Service Desk will be able to assist with technical advice where required. If you have any general queries, please contact the Information Manager on Ext. 5550.

5.17 Disposal of PCs

A PC may be permanently disposed of when it has reached the end of its useful life. Reasons for this may include:

- The equipment is faulty and beyond economical repair
- Specification is no longer adequate
- Incompatibility with other equipment

The S&S HIS need to confirm that a PC needs to be disposed of and will inform users of the information required to be noted on the disposal certificate. Please contact the S&S HIS Service Desk via the HIS Service Desk Portal on the Trust's Intranet homepage The S&S HIS will update the Trust's Asset Register of the disposal.

All equipment must be disposed of in line with the Trust's Condemned Equipment Policy - see Trust Intranet, Policies, Disposal of Surplus - Obsolete - Condemned Equipment Policy.

No data should be stored on the PC Hard Disk; however if any data needs to be removed the HIS engineer will be able to assist the user.

The S & S H I S have an arrangement with a specialist contractor for the safe disposal of PCs in line with EU regulations.

5.18 Portable Memory Sticks

Portable memory sticks plug into the USB port on a PC and can be used to store large amounts of data which together with their small physical size brings certain risks. The following measures must be taken.

- Only Trust owned and configured sticks are to be used
- Do not use them to store confidential data
- Ensure all data is removed from the stick before disposing of it
- Store memory sticks securely when not in use
- Do not rely on them to back up critical systems

Trust supplied memory sticks are centrally managed and meet NHS encryption standards. Use of any other USB storage devices is prohibited and may result in disciplinary action. Please contact the IT Operations Manager to apply for a memory stick. Please email AllysonJones@burtonft.nhs.uk

5.19 Software Copyright

The Trust licenses the use of computer software from the software suppliers. It is not owned by the Trust, and cannot be reproduced without authorisation from the software developer. Any copying of software without the copyright owner's permission is an infringement of the copyright law. The Federation Against Software Theft (FAST) is an association dedicated to tackling breaches of copyright. They have the right to come into organisations to check the law is being complied with.

If you are using illegal software, you are personally liable for the breach in addition to the Trust. Any employee found copying software, other than for legitimate backup purposes may be dealt with under the Trust's disciplinary procedures.

If you need to use software licensed by the Trust at home for work purposes, you must be sure that the licence for the program permits home use.

5.20 General Precautions

Do not locate PC's close to heat and water, e.g. radiators, pipes etc Cables

should be kept tidy and away from walkways

Do not allow drinks near to, or place plants on top of computer equipment

Paper must not be stored on or near to equipment due to risk of fire

Do not position PC screens where unauthorised persons can see personal information

Always exit from applications and shut down the PC properly

In order to save energy please turn off computer equipment whenever it is not going to be used for long periods (i.e. overnight and weekends).

6. DATA PROTECTION ACT

6.1 Introduction

The Data Protection Act 1998 applies to MANUAL as well as computer records and affects all staff across the Trust who have access to information about patients, staff, or other individuals.

The Act obliges the Trust to provide a brief description of this data, including uses, sources and disclosures to the Office of the Information Commissioner. Trust staff should contact the Trust's Data Protection Officer on Ext. 5550 if they have any queries.

Data users must follow eight internationally accepted "Data Protection Principles" on which the Act is based, and which together define a code for personal data. To ensure compliance, the Act establishes criminal offences if these responsibilities are neglected.

If unsure about your responsibilities, seek advice from the Data Protection Officer on Ext. 5550.

6.2 The Data Protection Act 1998 Principles

The Act specifies eight principles of good practice that must be complied with by users of personal data. Personal data is any information held manually or on computer that relates to a living individual.

1. *"Personal data shall be processed fairly and lawfully".*

   The common law duty of confidentiality must be complied with. The person must not be misled into giving the data and will be told who will use the data and for what purpose(s).

2. *"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".*

   Information obtained for one purpose cannot be used for another purpose without consent, unless there is an overriding public interest.

3. *"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".*

   Depending on the particular situation there may be Health Service and/or professional guidelines regarding the taking and making of records that must be followed.

4. *"Personal data shall be accurate and, where necessary, kept up to date".*

   The data must be correct, complete and timely.

5. *"Personal data processed for any purpose(s) shall not be kept for longer than is necessary".*

   Certain types of record must be kept for a minimum period laid down by law or NHS guideline.

6. *"Personal data shall be processed in accordance with the rights of data subjects under this Act".*
   These include the right of access to the information.

7. "Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

8. "Personal data shall not be transferred to a country or territory outside the European Economic Area (unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

   The data must not be sent outside Europe unless adequate controls are in place.

6.3 Access to Personal Data

An individual person is entitled to ask to see what information is held about them on computer and manual records. This right is subject to certain terms and conditions being met. It is an offence to refuse a valid request for access. The request must be dealt with within 40 days of receipt.

Requests for access are dealt with by the following:

- Health Records Manager on Ext. 5466 - for patient information enquiries
- Senior Human Resources Manager on Ext. 5715 - for payroll/personnel information

If the above are not applicable then please contact the Head of Legal Services on Ext. 5929.

Do not attempt to answer the request yourself, ensure it is passed on to the appropriate contact point.

6.4 Individuals' Rights

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

- Right to access the data
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes 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 request an investigation as to whether any part of the Act has been contravened

If you have any queries or concerns please contact the Data Protection Officer on Ext. 5550.

6.5 Information Asset Owners

The Trust is required to identify a responsible person for each system in the Trust. This role is designated as a "Data Custodian" under the Data Protection Act but is also known as an Information Asset Owner. This individual has responsibility for:

- System security
- Ensuring access is restricted to authorised users
- Notifying the Data Protection Officer of significant changes to data held
- Ensuring systems are used in accordance with relevant policy and procedures

For corporate systems (e.g. Meditech) security controls are mainly centrally administered, although there are some local responsibilities.

Where an Information Asset Owner has not been identified this role will be the responsibility of the Head of Department.

6.6 Safe Havens

Any area in the Trust that handles confidential person identifiable data (PID) will be regarded as a Safe Haven location.

The following security measures will apply:

- A Safe Haven Office should be locked or manned at all times
- The room should be situated so that only authorised staff have access, it should not be a room that allows access to other areas/departments
- Manual paper records containing PID should be locked when not in use
- Computers should not be left on view or accessible to unauthorised staff. They should have a screen saver function when not in use
- Fax's that are used for (PID) should be located in a Safe Haven, should have a code password and be switched off when not in use

Procedures

The Trust has developed procedures for all methods of transferring confidential information, which staff must adhere to:

- **Post** – see Postage and Mail Policy
- **Electronic / E-mail** – see Email Usage Policy – section 5.10 of this Policy
- **Transporting** where staff need to use an external courier or taxi firm – the Trust's approved courier service and taxi firms must be used

- **Faxing** – please see separate Fax policy. NB the Trust will cease using fax machines during 2018
- **Bulk Transfer** – please contact the Information department for assistance

6.7 Unauthorised Disclosure of Manual Patient Records

It is essential that all disclosures of confidential manual patient records are reported **promptly**. Examples of unauthorised disclosure are lost case notes.

The incident should be reported to your immediate supervisor and the Health Records Manager on extension Ext. 5466. In cases where it is your supervisor that is suspected then report it to the manager above.

The incident will be investigated by the Medical Records Manager. There is an escalation procedure to involve more senior staff in serious cases.

A log of incidents is kept, and is reviewed periodically to establish whether security measures need to be improved.

All staff are individually responsible for reporting such incidents.

7. TRAINING

For good Information Security it is essential that computer users are sufficiently trained so that they are aware of the risks to systems and the security measures available.

Information Security training is incorporated within the wider Information Governance Training Programme. General courses are available for all staff both on line via e-Learning and in classroom based sessions. It is the responsibility of Line Managers.

8. MONITORING AND REVIEW

Both compliance with and effectiveness of this Policy will be monitored by the Information Governance Steering Group on an ongoing basis. This will include a review of security incidents to determine whether further controls including policy change are required. Periodic reviews will be carried out by Internal Audit.