The Tavistock and Portman NHS
NHS Foundation Trust

Information Management & Technology Security Procedure

Version:	3.1
Bodies consulted:	-
Approved by:	PASC
Date Approved:	10.5.16
Lead Manager	Director of IM&T
Lead Director:	Deputy Chief Executive
Date issued:	May 16
Review date:	Apr 19

Contents

IM&T Security Procedure

1 Introduction

The Trust recognises the importance that all of its systems are protected to an adequate level from vulnerabilities. Such risks include accidental data change or release, malicious damage (internal or external), fraud, theft, failure and natural disaster. It is important that a consistent approach is adopted to safeguard the Trust's information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.

2 Purpose

2.1 As well as a common law duty of care, the Trust has a legal obligation to maintain security and confidentiality for the data it holds, including:

Data Protection Act 1998,

Computer Misuse Act 1990.

There are also regulatory requirements with which all NHS organisations must comply, including those set out in the Department of Health's Information Governance Toolkit, the NHS network (N3) and Statement of Compliance. It is the duty of the Trust and its staff members to meet these legislative and regulatory requirements in relation to IM&T Security.

This policy sets out the procedures to be followed by all Trust staff to ensure that the Trust's ICT assets — hardware, software and data — are protected and that the Trust's right to use the 'NHS network' is not compromised. It is aimed at ensuring:

Confidentiality: data access is confined to those with specified authority to view the data

Integrity: all systems are working as they were intended to work and all data protected from unauthorised change

Availability: data is available to the right person, when needed

2.2 The need for a Security Policy

Data stored in information systems represent an extremely valuable asset. The increasing reliance of the NHS on ICT for the delivery of health care makes it necessary to ensure these systems are developed, operated, used and maintained in a safe and secure fashion.

The increasing need to transmit information across networks of computers renders data more vulnerable to accident or deliberate unauthorised modification or disclosure. The use of computers to exchange data electronically offers advantages to NHS patients if handled securely, but could present serious hazards if security is inadequate.

3 Scope

This policy applies to all Trust staff (both permanent and non-permanent), students and contractors or staff employed by other organisations but working on behalf of the Trust.

It also applies to all areas of Trust 'business' so covers all Trust Information Assets, be they Patient related, or not.

The Trust has made a firm commitment to monitor and protect its confidential information. This may be person identifiable information relating to patients or staff members or it may be documents of a commercially confidential or sensitive nature. It has, therefore, become a fundamental principle of the Trust to have an effective and consistent Information Management and Technology (IM&T) Security Procedure in place.

4 Definitions

Abbreviation /Definition	Definition
ICT	Information Communication Technology
IT	Information Technology
IGT	Information Governance Toolkit
CG	Caldicott Guardian
Encryption	Process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Smartcard	A plastic card (like a credit card) with an embedded microchip for storing information. The NHS smartcard is used to control security access to electronic patient records.
SSSP	System Specific Security Policy, as it suggests is a policy detailing the ICT security arrangements for a specific ICT system.
BD	Board of Directors
SIRO	Senior Information Risk Owner

IGSOC	Information Governance Statement of Compliance - an agreement between the Trust and HSCIC for access to the NHS National Network (N3). The process includes elements that set out terms and conditions for use of HSCIC systems and services including the N3, in order to preserve the integrity of those systems and services.
HSCIC	Health and Social Care Information centre — The Body managing ICT within the NHS and informatics
Information asset	See the Trust's *Information Asset Acceptance and Registration Procedure*

5 Duties and responsibilities

5.1 Chief Executive

The CE has ultimate responsibility for all elements of Governance be it Clinical, Information or Corporate. The CE has delegated the task of overseeing all Information Governance related issues to the Senior Information Risk Owner (SIRO).

5.2 Senior Information Risk Owner (SIRO)

The Trust's Senior Information Risk Owner (SIRO) has overall responsibility for all aspects of information Governance. The post holder is an executive director appointed by the Board of Directors (BD). The SIRO reports to the BD through the Corporate Governance and Risk work stream.

5.3 Caldicott Guardian

The Caldicott Guardian is the Trust adviser with respect to the protection and use of patient information. The post holder has an overarching responsibility in relation to the confidentiality and security of Patient Information and assists in the formulation of related policies and procedures. They also provide expert training and advice to staff.

5.4 Information Governance Lead

The IG lead must ensure that this policy, as well as any supporting documentation, is accurate and relevant to the Trust's situation in relation to Information Governance.

5.5 Director of IM&T

The Director of IM&T is responsible for ensuring the implementation of this procedure throughout the Trust. The director will also authorise the procurement/ acquisition of minor

5.6 ICT Security Lead

This is the ICT Manager and is supported through the IM&T Management Committee, chaired by the SIRO. Duties include:

- Periodically report to the IM&T Strategy Board the state of IM&T security within the organisation
- To keep up to date with new developments and requirements to ensure the Trust's IM&T security policy remains current
- Liaise with the Trust IG Lead to ensure the policy and any related procedures meet any required standards
- Ensure that IM&T security policy is implemented to at least the level laid out in the NHS IM&T Security Manual
- Ensure compliance with relevant legislation including the Data Protection Act (1998), Computer Misuse Act (1990) and Access to Health Records Act (1990)
- Help ensure that all staff are aware of their security responsibilities by assisting with regular IM&T security awareness training and providing support and guidance for all users
- Assist with Internal Audit plans to review the Trusts' compliance with local and NHS security policies
- Authorise all software purchases in the Trust.

5.7 Information Asset Owners (IAOs)

IAOs will be responsible for discharge of this procedure for their assets (especially sections 7 & 8), see Information Asset Acceptance and Registration Procedure for more information.

5.8 All Staff

All staff employed by the Trust are responsible for ensuring that they comply with the Trust's information governance requirements, including ensuring they apply the standards set within the IM&T Security policy.

6 Procedures

The Trust will maintain an inventory of the physical assets associated with its information systems; this will include:

6.1 Physical Assets

Each physical asset will be assigned an "owner". The owner of all physical assets (computer hardware and associated peripheral equipment) is the Trust but for practical purposes (security marking, inventory, maintenance etc.) this is delegated to the ICT Manager.

6.2 Software Application Assets

The ICT Manager will also be responsible for maintaining a register of all software applications deployed within the trust, including ensuring the Trusts holds copies (or evidence) of relevant licences.

6.3 Access Control

A key element of IM&T Security is ensuring suitable controls are in place to restrict access to those who actually need it. Also, it is important to ensure that measures are in place to prevent misuse or theft of the relevant assets.

6.4 Trust systems

The ICT Manager is responsible for the leading on security for all the Trust-wide electronic systems, including the maintenance and developments of related procedures and policies.

Special attention will be given to the allocation of "privileged" or "supervisor" rights, which will normally be available only to certain members of the IM&T department on a 'need to know' basis.

Identification which satisfies the government recommended standard 'e-Gif Level 3', providing at least three forms of ID (photo and non- photo), including proof of address is a pre-requisite for access to any Connecting for Health systems and is undertaken by Human Resources as part of the Trust's recruitment procedures.

6.5 Gaining access

To access to any 'Information Asset' the user must first have an authorised and active Trust user account, which will be managed by the ICT Department. The ICT Manager (this may be devolved to members of the ICT team or Information Asset Owner/Administrator for other assets) will:

- check that the level of access requested is consistent with organisational security policies
- keep a record of all users
- remove the access rights of any staff who have changed jobs or left the organisation [1]
- periodically check for and remove redundant user IDs and accounts that are no longer required
- ensure that redundant user IDs are not re-issued to another person.
- all users' access rights will be reviewed periodically to ensure
- that access levels remain consistent with their duties.
- all new staff should be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected as part of the staff induction process.

Access to computer services and data will be controlled on the basis of business requirements and is the responsibility of the ICT Manager in cooperation with the data "owner" and relevant managers. Levels of access will be set by the ICT Manager (or Information Asset Owner/Administrator for specified assets) to allow access to sensitive areas within a system or allow the user to undertake general user account management and system configuration.

6.6 Password Management

The ICT Manager (or Information Asset Owner/Administrator for specified assets) will implement, where possible, automated password systems to authenticate users. Each member of staff will have their individual user identification and password. Passwords should not relate to the user or to the system being accessed. The ICT Manager (or Information Asset Owner/Administrator for specified assets) shall:

- enforce the use of individual passwords to maintain accountability. The use of 'team' passwords may be necessary for access to email in certain circumstances.
- allow users to select and change their own passwords and include a confirmation procedure to allow for typing errors
- enforce a complex password (letters, numbers and special characters) with a minimum length of 7 characters for passwords. NB: ICT is recognised that hackers using "password cracking" software are capable of using a great many password probes in a short space of time. The most effective passwords are therefore those with the longest character string.
- enforce a password change at 30 day intervals (users will be automatically prompted when password renewal is due)
- maintain a record of at least the last 5 previously used passwords and prevent users from re-using them
- **not** display passwords on the screen when being entered
- limit the number of unsuccessful log-on attempts to 3, after which: the account is locked; the user must contact the ICT Helpdesk before system access can be re-instated.

[1] Dependant on being informed via monthly leavers list from HR or department managers upon the change of staff status

The Password "time-out" facility within Windows will be implemented for all staff to avoid unauthorised access when staff members are temporarily absent from their workstation.

6.7 New starters, leavers and movers

Starters

- All new accounts together with required access are to be requested by the employee's manager using the new staff request form; this can be obtained from the Intranet or the ICT Helpdesk.
- The manager will complete the form and submit it to the ICT helpdesk
- The new user account is created in Active Directory (AD)
- Confirmation that the new account details have been set up will be sent to requesting manager

Movers and leavers

- Section managers/HR should notify the ICT helpdesk by email if a member of staff is moving departments or leaving as soon as it is possible to do so (HR will provide a monthly leavers list for action).
- The ICT Helpdesk will disable a user's account within 1 week of receiving the leavers list unless a specific request is made for faster action, accounts will be deleted after 3 months. Requests to maintain a leaver's account after they have left must be submitted in writing by an authorised manager.

6.8 Equipment Security

The ICT Manager will ensure that:

- all Trust PCs and laptops are installed with endpoint security software, allowing ICT to control which external storage devices can connect to the Trust network. This measure ensures that only authorised devices can be used for copying data to/from the Trust network
- equipment to be used outside of the Trust network (including all laptops and tablets) is installed with a suitable encryption agent to protect the data held therein
- only Trust approved USB memory keys are permitted read/write access on the network. These keys are encrypted on first use. Non-Trust or unencrypted memory keys will only have read access
- critical equipment is protected from power failures through use of uninterruptible power supplies (UPS). These systems will warn of electrical failures and automatically initiate orderly shutdown if power is not restored within a specified time
- any maintenance arrangements that are the subject of contractual agreement have only approved system engineers accessing
- in general terms, fileservers, routers and other computer hardware, critical to the effective running of the network are the subject of maintenance contracts, whilst individual end computing devices are not (it being cheaper

to replace failed equipment than to maintain it under contract)

- where there is uncertainty as to whether an individual hardware item should be the subject of a maintenance contract or not, the ICT Manager will undertake a risk assessment of the loss of availability

- Records are kept of all faults on centrally maintained equipment

Hard disks containing Trust data are not be removed from the premises (other than in laptops or PCs being deployed or returned to the ICT department for repair) without the written authorisation of the Director of IM&T. Actual removal will be overseen by the ICT Manager.

Any storage media (e.g. external hard disks, USB keys) should be disposed of only after reliable precautions to destroy the data have been taken. The procedures taken for disposal of PCs deemed excess to requirements must be documented and "signed-off" by the ICT Manager.

Media which has held particularly sensitive data, e.g. patient identifiable data, must be physically destroyed. This will be overseen by the ICT Department but may be done by third party agencies under strict licence. Certificates of destruction must be provided by the agency responsible and a record maintain by the ICT Manager.

NB simply deleting data from disks is not adequate as "delete", "erase" and "format" commands are all processes that can be reversed. Hard disks should be over-written with randomly generated characters using software specifically designed for this purpose, or physically destroyed. Detailed procedures governing the safe disposal of old equipment or wiping of discs are available from the ICT Department

6.9 Network Security

The Trust has agreed the Information Governance Statement of Compliance (IGSOC). This is the process by which organisations enter into an agreement with HSCIC for access to the NHS National Network (N3). The process includes elements that set out terms and conditions for use of NHS systems and services including the N3, in order to preserve the integrity of those systems and services.

The ICT Manager will be responsible for ensuring continued compliance with the Code of Connection which can be summarised as follows:

- The Trust will abide by the NHS-wide Networking Data Security Policy;
- access to NHS-wide networking is protected by at least one authentication control e.g. network access password;
- one named individual (the IM&T Security Officer) is made responsible for the security of any system or network connecting to the NHS-wide infrastructure;
- all relevant staff are made aware of their responsibilities in relation to the security of the NHS-wide infrastructure;
- physical access to all NHS-wide network termination equipment is controlled;

- all incidents which constitute a threat to NHS-wide networking services are reported to the HSCIC as and when they occur;
- commercial advertising or any other form of promotional activity for non-NHS purposes is forbidden;
- any system connecting to the NHS-wide networking infrastructure is managed according to the requirements of the NHS Top Level Security Policy published with EL (92) 60 and in accordance with all security guidelines issued by HSCIC;
- where direct on-line access to NHS systems is allowed, staff are made aware of the additional care required;
- all program files obtained through connection to external services are checked by a virus checking facility and approved by a Technical Manager before being used on any system connected to the NHS- wide networking infrastructure;
- if the Trust provides a permanent host system on the Internet or any related service, there shall be no connection between the host system and NHS-wide network services

The Trust will undertake an annual audit to ensure compliance with the code of connection.

6.10 ICT Security Incident Management

ICT Security incidents will be reported and managed under the Trust's Incident Reporting Procedure; this procedures can be found on the Trust's website

6.11 System Planning, Procurement and Acceptance

Acquisition of any new 'ICT asset must conform to all standards set out within this policy and relevant Standing Financial Instructions. All security requirements should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

Major applications etc will be considered by the Information Management and Technology Strategy Board. Minor applications will be considered by the ICT Manager –see appendix B.

Prospective Information Asset Owners and those responsible for software must liaise with the ICT Manager to ensure that:

- hardware or software changes which may affect network management are agreed by all parties affected.
- any new ICT facilities provide an adequate level of security and will not adversely affect existing security
- mandatory, as defined above, and desirable security requirements are included in procurement specifications
- Access controls and User Management, appropriate to the purpose and content of the new asset, should be included in the procurement specification.

- Suitable back-up and disaster recovery procedures will be in place
- Training requirements are considered for any new hardware and software involved in the new asset, both for local management and IM&T support
- set documented user acceptance criteria against which the system can be tested.

Project approval may be withheld until the all above elements have been built into the project plan and agreed**6.12 Remote Access**

Remote Access is defined as access to the Trust's ICT systems and services from any location other than a site owned and/or operated by the Trust e.g. home working or another NHS site.

Remote Access Principles

In providing remote access to staff, the following high-level principles will be applied:

The ICT Manager will be appointed to have overall responsibility for each remote access connection to ensure that the Trust's Procedure and standards are applied.

A formal risk analysis process will be conducted by the ICT Manager for each application to which remote access is granted to assess risks and identify controls needed to reduce risks to an acceptable level.

Remote users will be restricted to the minimum services and functions necessary to carry out their role.

Eligibility

Trust staff may apply for Remote Access by completing a Remote Access Request Form if they satisfy the following conditions:

- They have a contract of employment
- Staff have a valid network username, password and email account
- A request form is completed, and approval by the relevant manager.
- Staff have read and acknowledged the relevant policies and agree to be bound by those policies by signing an undertaking.

Contractors and other support/service staff (i.e. system proprietors) who may require access in the course of providing system support and maintenance can be granted access once they have signed the Confidentiality Agreement for Contractors.

That access will be restricted to the minimum necessary for the user to be able to carry out their duties safely.

Registration

All remote users must be registered and authorised by the ICT Manager. User identity will be confirmed by strong authentication and User ID and password authentication. The Trust's ICT Manager is responsible for ensuring a log is kept of all users Remote Access.

ICT is the responsibility of the ICT Manager who will ensure that robust administration and filing procedures are in place so that user access is strictly controlled and that this can stand up to detailed audit.

Security Technologies

To ensure comprehensive protection, every network will include components that address the following 5 aspects of network security:-

User identity will be confirmed by strong authentication and User ID and password authentication. The ICT Manager is responsible for ensuring a log is kept of all user remote access.

Perimeter Security - The ICT Manager is responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches handle this access control with access control lists and by dedicated firewall appliances. Remote Access Systems with strong authentication software control remote dial in users to the network. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organisations deploy to improve their security postures.

Secure Connectivity - The Trust will protect confidential information from eavesdropping or tampering during transmission.

Security Monitoring - Network vulnerability scanners will be used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

Remote diagnostic services and 3rd parties

- Suppliers of central systems/software expect to have remote access to such systems on request to investigate/fix faults. The Trust will permit such access subject to it being initiated by the computer system and all activity monitored.

- Each supplier or Trust user requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives.

- Each request for remote access will be authorised by approved IM&T staff, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed/supplier ends his session.

- User Responsibilities, Awareness & Training - The Trust will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s).

- Reporting Incidents & Weaknesses - All security weaknesses and incidents must be recorded and reported via the Trust Risk Management Procedures for assessment, with action taken as appropriate.

6.13 Mobile Devices

Portable and mobile devices, e.g. laptop computers, smart phones and tablets, taken outside secure NHS environments are subject to special security risks: they may be lost or stolen and may be exposed to unauthorised access or tampering. Laptops and other devices taken abroad may also be at risk, for example confiscated by police or customs officials.

Mobile device loss will mean not only the loss of availability of the device and its data, but may also lead to the disclosure of patient or other sensitive information. This loss of confidentiality, and potentially integrity, will often be considered more serious than the loss of the physical asset.

Where large quantities of NHS data are held on a single laptop (or other storage medium) risk assessments must consider the impacts of loss of all the data. Note that deleted files should be assumed to persist on the laptop's hard disk.

Some Key Points

- Traditional password protection on a mobile device offers limited defence against a determined attacker because the attacker has unconstrained access to the physical device.

- The physical security controls that are possible within an NHS buildings environment are not available outside of that environment; therefore if procedural and personal controls of the device are breached the only effective technical measure that can be applied is cryptography. CESG provide guidance on laptop protection, evaluated products and other good practice which if followed provides an adequate level of security. This is available through the CESG website at www.cesg.gov.uk

- Encrypted products are not difficult but must be used correctly in accordance with defined procedures, in particular the password and any token must be kept

separate from the mobile device; these are effectively the encryption key. Data is therefore only protected by encryption when the laptop is powered off and not in normal use.

Unauthorised Access

Unauthorised access and tampering to a mobile device, particularly if there are repeated opportunities for access, may:

- lead to continuing (and undetected) compromise of information on the device itself;
- undermine security measures (including the encryption); intended to protect information on the device in the event of loss or theft; and
- lead to compromise systems to which the device is connected, for example, an NHS organisation's networked systems that are accessed from the device under an approved remote access arrangement
- The impact of a breach of device security may therefore extend far more widely than the device itself.

NHS Information Security Principles and Policy

ISO/IEC 27002, Code of practice for information security management, the NHS Information Security Management Code of Practice, and the NHS Information Governance Toolkit set out principles relevant to mobile device protection; assurance that these standards are being met will be measured through the IG toolkit reporting to the IG workstream group.

Baseline Information Security Standards

The following information governance principles and policy will apply when using mobile devices:

Registration

- All mobile devices used for Trust business or holding Trust information must be uniquely identified and registered in the Trust's asset register. Registration/enrolment is carried out with a Mobile Device Management (MDM) platform for all non-Windows devices.
  Trust owned Windows devices will be deployed with Microsoft Direct Access technology.

Management of mobile device security functionality

- The installation and configuration of mobile device security functionality, including access control, encryption, remote presence and tamper resistance will be undertaken by appropriately trained staff within the ICT Team.

User training and awareness

- Users of mobile devices will be given appropriate training and instruction in the use of the device and its security functionality by ICT staff. This should include their responsibility for safeguarding the device and their obligation to comply with relevant information security procedures.

Security accreditation

- The ICT Manager will regularly review the NHS organisation's mobile device estate to ensure that they continue to meet these requirements and that the residual level of risk from their use is acceptable. This could be done by sample audit to ensure all mobile devices continue to be logged on the asset register and contain the relevant encryption solution.

Remote Access

- Remote access from a laptop to NHS information systems must be achieved in accordance with the organisation's NHS IG Statement of Compliance, NHS IG guidance, and any defined requirements for the protection or use of the NHS information service(s) concerned.

Data Storage and use

- Sensitive data, including that relating to patients, stored on an NHS laptop should be kept to the minimum required for its effective business use in order to minimise the risks and impacts should a breach occur.

Incident Reporting

- Loss of NHS laptops should be reported as a Serious Untoward Incident in accordance with the Trusts incident management and reporting arrangements. Details of these arrangements are available to all users via the Trust Intranet.

Physical security measures to be taken by all users

- When in use, mobile devices should never be left unattended, especially when working off-site. Make use of room locks and lockable storage facilities where available.

- Where the mobile device must be left for a few hours or overnight it should be logged off and stored in a locked drawer or cabinet.

- All removable media such as CD-ROM, floppy disk drives and USB keys should be disabled or removed unless absolutely necessary.

- When travelling and not in use, ensure that mobile devices are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the

boot. Mobile devices left on display and unattended will inevitably attract attention and are likely to be stolen.

- Do not leave mobile devices unattended in car boots overnight.

- When travelling, avoid placing mobile devices in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots.

- Be aware that the use of mobile devices in public places is likely to draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

- Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc and on public transport e.g. buses and trains.

- It is good practice to carry mobile devices in protective anonymous bags or cases (i.e. those without manufacturer logos on them) when not in use

Logical security measures to be taken by ICT and supported by users

The ICT Manager will ensure that the following are applied:-

- Full disk encryption will be deployed on all Trust issued laptops/compatible tablets (i.e. Windows tablets).

- Where full disk encryption is not possible, an acceptable form of encryption should be provided at file or directory level to enable sensitive data to be encrypted whilst at rest

- Laptop BIOS passwords should be used to prevent BIOS settings being changed

- Trust laptops/compatible tablets will be configured so that they cannot be booted from external media when in normal use

- Implement procedures and processes in relation to the provision and maintenance of anti-virus and other security software on laptops/compatible tablets, 'lockdown' of the desktop on laptops and other appropriate measures

- Tamper-proof labels should be fitted to laptops and tablets for asset identification, and to disk drives and ports which should not be used

- All laptops/compatible tablets that have been off the network for up to 30 days have to be returned to ICT as soon as possible **before** being used on the network. This is to perform a network health check and to ensure all security software and OS patches are up to date.

- Trust smartphones, tablets (iOS, Windows) will be registered and managed by the MDM solution. Blackberry's will be managed with Blackberry Enterprise Server (BES).

7 Training Requirements

These procedures reinforce many of the requirements set out in policies such as Data Protection policy and Access to Health Records Policy and Records Retention Policy. All staff will receive awareness training as set by the Management Team.

Staff will also receive training in any specific systems they will use as part of their role. Training here will be the responsibility of the Information Asset Owner/Administrator for that system.

Finally, training will be further re-enforced via the annual IG Training requirements within the IGT

8 Process for monitoring compliance with this Procedure

Effectiveness will be monitored by the Head of Informatics and the ICT Manager who will regularly report to the IM&T Management Committee.

9 References

Data Protection Act 1998

Freedom of Information Act 2000
NHS Care Record Guarantee
Code of Practice for the Management of Records

NHS employers Identity Checking Guidelines

Information Governance Statement of Compliance (IGSOC)

NHS Information Management & Technology Security Manual

The Power of Information. (2013). Department of Health: London.

10 Associated documents[2]

[2] For the current version of Trust procedures, please refer to the intranet.

Code of Conduct on Patient Identifiable Information (Confidentiality)
Health Records Procedure
Data Protection Procedure
Corporate Records Procedure
Freedom of Information Procedure
Serious Incident Procedures
Incident Reporting Procedures
Information Asset Acceptance and Registration Procedure
Staff Safety and Security Procedure

Appendix A : Equality Impact Assessment

Completed by	**Jonathan McKee**
Position	**Governance Manager**
Date	**6.5.16**

The following questions determine whether analysis is needed	**Yes**	**No**
Does the policy affect service users, employees or the wider community? The relevance of a policy to equality depends not just on the number of those affected but on the significance of the effect on them.	X	
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?	X	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		X

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then undertake the following analysis:

	Yes	**No**	**Comment**
Do policy outcomes and service take-up differ between people with different protected characteristics?		X	

What are the key findings of any engagement you have undertaken?			Na
If there is a greater effect on one group, is that consistent with the policy aims?		X	
If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?			Na
Will the policy deliver practical benefits for certain groups?	X		Likely to enhance data security and enhance confidence for groups anxious about privacy.
Does the policy miss opportunities to advance equality of opportunity and foster good relations?		X	
Do other policies need to change to enable this policy to be effective?		X	
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 – seek advice from Human Resources (for staff related policies) or the Trust's Equalities Lead (for all other policies).

Appendix B : the acquisition of software to process non-personal data

Desktop Software

Standard software such as MS Office, MS Project, and MS Visio etc will be selected by the IM&T Director.

One-off software must be first should be tested to ensure it meets all Trust requirements (security, IG, compatibility, ICT support capacity and capability etc) then if both the ICT Manager and the requestor wish to pursue the acquisition then it can be procured in the usual way. Should the requestor wish to pursue a prospective acquisition that the ICT Manager has rejected then they may put their case to the Director of IM&T for a final decision.

Requests for software duplicating existing products will be declined; however, such requests may be considered when the existing software is due for renewal.

Server based software, eg *CareNotes*, *Meeting Manager* etc…,

It is likely that such products will process personal data. Those that process personal data will be assessed according to the Information Asset Acceptance and Registration Procedure. All proposed information assets will be considered by the IM&T Steering Committee for the final decision.

All other software will be considered in the way the desktop proposals are considered if they only are to be used by a small number of users and do not require significant ICT resources. More substantial products will be considered by the IM&T Director.

Procurement process

All ICT software or hardware must be processed through ICT on SBS, partly to conform to SFIs and partly to ensure that ICT know to expect the delivery and manage the installation.