Somerset Partnership NHS
NHS Foundation Trust

INFORMATION SECURITY POLICY

This policy should be read in conjunction with the:
Information Governance Policy
Confidentiality and Data Protection Policy
IM&T Use by Service Users/Carers of IT Equipment

Version:	6
Ratified by:	Senior Managers Operational Group
Date ratified:	April 2015
Title of originator/author:	Information Technology Technical Architect
Title of responsible committee/ group:	Caldicott and Information Governance Group
Date issued:	October 2015
Review date:	March 2018 CIGG agreed to extend to May 2018
Relevant Staff Groups:	All Staff

This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity Lead on 01278 432000

DOCUMENT CONTROL

Reference KH/Apr15/ISP	**Version** 6	**Status** Final	**Author** Information Technology Technical Architect
Amendments	Incorporated policy to integrate all IM&T policies eg Bulk Transfer of Data, Data Quality and Mobile Working and Remote Access		
Document objectives: To provide Somerset Partnership NHS Foundation Trust with robust advise on implementing information technology			
Intended recipients: All Staff			
Committee/Group Consulted: Caldicott and Information Governance Group			
Monitoring arrangements and indicators: Caldicott and Information Governance Group			
Training/resource implications: Please refer to section 6			
Approving body and date	Caldicott and Information Governance Group	Date: January 2015	
Formal Impact Assessment	Impact Part 1	Date: March 2013	
Clinical Audit Standards	NO	Date: N/A	
Ratification Body and date	Senior Managers Operational Group	Date: April 2015	
Date of issue	**October 2015**		
Review date	**March 2018** CIGG agreed to extend to May 2018		
Contact for review	Information Technology Technical Architect		
Lead Director	Director of Governance and Corporate Development		

CONTRIBUTION LIST Key individuals involved in developing the document

Name	Designation or Group
Kurt Hanson	Information Technology Technical Architect
All Members	Caldicott and Information Governance Group
All Members	Senior Managers Operational Group
Andrew Sinclair	Equality and Diversity Lead

CONTENTS

1. INTRODUCTION

1.1 Information can exist in many forms: written or printed on paper, stored electronically, shown on film or spoken in conversation. This document describes the Somerset Partnership NHS Foundation Trust Information Security Policy requirements for all information and information systems.

1.2 This document sets out the overall policy for the security of the Trusts information assets and the information contained on or within.

1.3 All process and risk specific policies will be referenced to this document, and will contain where appropriate, a policy statement, procedure, standards, guidelines and baseline documents. See Section 9.

1.4 The policy and associated documents are intended to deliver Trust compliance with both best practice and the requirements of the NHS Information Governance Toolkit, which includes the standards set by Caldicott guidance and legislation.

1.5 The legal framework is included as Appendix K.

2. PURPOSE & SCOPE

2.1 This policy and associated documents apply to all Trust staff that access and use any of the Information Systems provided for them to perform their role within the organisation. Additionally this applies to all staff, and people not employed by the Trust but working on behalf of the Trust, for example in integrated teams, secondees, agency and temporary staff. ‘Staff’ from here on in this policy includes all these people.

2.2 It covers access to these systems from external locations such as other Healthcare environments, partner organisation and home access.

2.3 It also covers access to non-trust systems such as the Internet when accessed from within the Trust.

2.4 It applies to all computer equipment that is used such as Servers, PCs, laptops, other mobile devices and any piece of information technology equipment that holds of processes Trust-related data.

2.5 It is recognised that some pieces of Medical equipment can and do hold data, which cannot necessarily be secured in the same way. Where this is the case, IM&T should be contacted (see security organisation section) so that advice on best practice can be given.

3. DUTIES AND RESPONSIBLITIES

3.1 Chief Executive

The Trust Chief Executive is the senior accountable officer for the enforcement of this policy. The Director of Finance and Business Development has delegated functional responsibility.

3.2 **Trust Board**

The Trust Board has overall responsibility for all matters relating to information security. All matters concerning security should be referred to the Trusts Caldicott Group and Information Group, which reports to the Integrated Governance Committee.

3.3 **Caldicott and Information Governance Group (CIGE)**

This is chaired by the Director of Nursing and Patient Safety/Caldicott Guardian, and is responsible for ensuring that all information security issues are cascaded into the operational divisions, by maintaining a list of IG Leads, who will be responsible senior managers. IGG shall ensure that this policy and all associated documents are updated and reviewed within the determined time schedules

3.4 **Caldicott Guardian**

3.5 The IM&T Department and any contracted third parties has the responsibility of ensuring that all policies and associated Standards and Guidance documents are adhered to.

3.6 All users are responsible for reporting incidents and weaknesses in breach of the Information Security Policy to the information technology department and / or the Somerset Partnership NHS Foundation Trust Information Governance department and through the Trust formal incident management procedure.

3.7 Information Asset Owners are responsible for ensuring that all staff are adequately made aware and/or trained to meet their responsibilities.

3.8 All Managers shall ensure that all external contractors and agencies working on behalf of the Trust are compliant with the Information Security Policy and all associated Standards and Guidance.

4. EXPLANATIONS OF TERMS USED

4.1 This Policy covers information that is in all formats: written or printed on paper; stored electronically, including emails; shown on film (DVD); spoken (digital dictation).

Term	Definition
IGTK	Information Governance Toolkit
CIGG	Caldicott and Information Governance Group
Information asset	Information in any form is an asset to the Trust – includes paper; electronic (email); CCTV images; voice recordings
Key information asset	A key information asset is one which supports the Trust's delivery of care
PID	Personal Identifiable Information
IAO	Information Asset Owner
IAA	Information Asset Administrator
SIRO	Senior Information Risk Owner
DPA	Data Protection Act 1998
Confidentiality	Ensure that information is accessible only to those

	authorised to have access
Integrity	Safeguard the accuracy and completeness of information and processing to insure confidence in the authenticity of the information
Availability	Ensure that authorised users have access to information and associated assets when required

5. MAIN POLICY

5.1 The Trust will ensure that all information systems are secure and all information is stored in accordance with NHS Guidance, Caldicott Guidance and the Data Protection Act 1998 (DPA) – see Appendix K.

It is the policy of the Trust that all information is protected against unauthorised access, ensuring confidentiality, integrity and availability of information. This will be managed by the Suite of Policies identified in specific areas in the appendicies.

5.2 Physical Security

All access to confidential and/or sensitive information (whether in hard copy or on computers) located within Trust property must be restricted through the use of the same precautions that are taken for other valuable assets of the Trust. Such restrictions include perimeter security, making sure that security doors are closed properly, blinds drawn, and that any door entry codes are changed regularly.

Staff must carry and preferably wear identification badges and wherever practical should challenge individuals not wearing identification in areas they know are not for public access. In such areas, visitors should be met at reception points and accompanied at all times and unaccompanied visitors should be taken out of the controlled area or to the Trust employee they are visiting.

Computers that are used to access confidential information should be located in rooms that have lockable doors or if not possible should be secured to the desktop. In the case of laptops these should be encrypted and stored securely out of sight overnight. Staff on termination of employment or contract must surrender door keys.

An unlocked and unattended workstation or computer is an easy target of unauthorised access. The Somerset Partnership NHS Foundation Trust IM&T department are to use computer policy to ensure password protected screen savers are invoked after an agreed number of minutes to ensure computers are locked when staff are inadvertently taken away from their screens for an extended period of time. Whenever a user leaves a workstation or computer, “Ctrl/Alt/Delete” or “Flag/L” must be used to lock the computer.

All computer assets including hardware and software must be recorded on an asset register that details the specification, user and location of the asset. The asset register must be regularly updated by. Each machine will be security

marked and its serial number recorded. Refer to the Information Asset Register Handbook for details.

Non-portable IT equipment must not be moved without checking on the suitability of the move with the IT Service Desk in advance.

Computers (whether supplied by the Trust or a personal laptop or computer) must not be connected to any network, including the Internet, without the permission of the IT Service Desk.

The IT Service Desk – 0300 3230111 must be notified of all computer equipment removed off-site. When removed from Trust's premises the user must take all reasonable care whilst in their possession. In particular, equipment must not be left visible in unattended cars, or on open display, this also applies if used at home.

Any theft, suspected theft, actual or suspected misuse must be reported as per the Trust incident reporting procedure, and your line manager must be informed.

Employees should make every effort to minimise the risk that fire, flood and accidents do not damage machines.

Equipment must be sited to minimise the risk of accidental damage. Common hazards include drinks cups, food and overstraining of leads when a machine is moved. Any suspected damage, which may not be visible externally (for example after dropping a computer), must be reported to the IT Service Desk for checking before continued use.

5.3 Disposal of equipment and media

5.3.1 Computer assets must be disposed of in accordance with the relevant IT Service desk disposal procedure. This includes removable computer media, such as tapes and disks and printed reports.

5.3.2 All redundant data storage devices will be purged of sensitive data before disposal. Where this is not possible due to quantities involved, the equipment or media will be destroyed by a technical waste service provider. Somerset Partnership NHS Foundation Trust IM&T have a contracted service for the disposal of IT equipment.

5.4 Use and installation of software

5.4.1 Under no circumstances should software, other than that approved and authorised, be loaded onto Somerset Partnership NHS Foundation Trust computers. Employees must not bring or download software onto the Somerset Partnership NHS Foundation Trust equipment without first gaining permission from the IT Service Desk.

5.4.2 It is a criminal offence in accordance with Appendix H to make/use unauthorised copies of commercial software and offenders are liable to prosecution and/or Somerset Partnership NHS Foundation Trust disciplinary procedures, which could result in dismissal.

5.4.3 "Games" software, except for the purpose of authorised educational purposes for staff or clients, is not permitted for use on Somerset Partnership NHS Foundation Trust equipment and must not be installed or used on the premises.

5.5 Incident management

5.5.1 Reporting information security incidents and suspected incidents is mandatory. All incidents must be reported using the Trust's incident reporting system (Datix). The Trust will investigate all suspected/actual security breaches and report to the Information Commissioners Office as per the incident reporting procedure.

5.5.2 All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions or negligence.

5.5.3 The Information Governance Manager and Senior Information Risk Owner must be informed of all unresolved security issues in order to carry out the appropriate investigation, as per the Trust incident procedure.

6. TRAINING REQUIREMENTS

6.1 The Trust will work towards all staff being appropriately trained in line with the organisation's Staff Mandatory Training Matrix (training needs analysis). All training documents referred to in this policy are accessible to staff within the Learning and Development Section of the Trust Intranet.

7. EQUALITY IMPACT ASSESSMENT

All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. In addition, the Trust has identified Learning Disabilities as an additional tenth protected characteristic. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Lead who will then actively respond to the enquiry.

8. MONITORING COMPLIANCE AND EFFECTIVENESS

8.1 Process for Monitoring Compliance

The following table outlines how the Trust will monitor compliance with the key elements of this policy.

Element to be monitored	Tool	Frequency	Reporting arrangements
Information Security Incidents	Datix	Quarterly	Caldicott
Compliance with the IGTK	National IGTK	X3 a year	Caldicott

9. COUNTER FRAUD

9.1 The Trust is committed to the NHS Protect Counter Fraud Policy – to reduce fraud in the NHS to a minimum, keep it at that level and put funds stolen by fraud back into patient care. Therefore, consideration has been given to the inclusion of guidance with regard to the potential for fraud and corruption to occur and what action should be taken in such circumstances during the development of this procedural document.

10. RELEVANT CARE QUALITY COMMISSION (CQC) – Regulation Standards

10.1 Under the **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Part 3), the fundamental standards** which inform this procedural document, are set out in the following regulations:

Regulation 9:	Person-centred care
Regulation 10:	Dignity and respect
Regulation 11:	Need for consent
Regulation 12:	Safe care and treatment
Regulation 13:	Safeguarding service users from abuse and improper treatment
Regulation 15:	Premises and equipment
Regulation 16:	Receiving and acting on complaints
Regulation 17:	Good governance
Regulation 18:	Staffing
Regulation 19:	Fit and proper persons employed
Regulation 20:	Duty of candour
Regulation 20A:	Requirement as to display of performance assessments.

10.2 Under the **CQC (Registration) Regulations 2009 (Part 4)** the requirements which inform this procedural document are set out in the following regulations:

Regulation 18:	Notification of other incidents

10.3 Detailed guidance on meeting the requirements can be found at http://www.cqc.org.uk/sites/default/files/20150311%20Guidance%20for%20providers%20on%20meeting%20the%20regulations%20FINAL%20FOR%20PUBLISHING.pdf

Relevant National Requirements

Information Governance Toolkit

11. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

Cross reference to other procedural documents

Confidentiality and Data Protection Policy
Hand Hygiene Policy
IM&T Use by Service Users/Carers of IT Equipment Policy
Information Governance Policy
Learning Development and Mandatory Training Policy
Record Keeping and Records Management Policy
Risk Management Policy and Procedure
Staff Mandatory Training Matrix (Training Needs Analysis)
Untoward Event Reporting Policy and procedure

All current policies and procedures are accessible in the policy section of the public website (on the home page, click on 'Policies and Procedures'). Trust Guidance is accessible to staff on the Trust Intranet.

12. APPENDICES

12.1 For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such. This should include any relevant Clinical Audit Standards.

Appendix A	Security of USB Equipment.
Appendix B	Authorisation for System Access
Appendix C	Dealing with Sensitive Information
Appendix D	Installation and Security of Software Applications
Appendix E	Use of Trust Equipment and Portable Devices
Appendix F	Network Shares
Appendix G	Email and Internal Usage
Appendix H	Bulk Transfer of Information
Appendix I	Data Quality
Appendix J	Procurement
Appendix K	Legal Framework for Information Security Policy
Appendix L	Remote Working
	(i) Mobile Working Code of Conduct
	(ii) Risks
Appendix M	Safe Haven and Fax Procedures

APPENDIX A

SECURITY OF EQUIPMENT

A1. Equipment Security

- All Trust Laptops, Mobile Devices and at risk Desktops are encrypted through the use of encryption software to render systems useless in the event of theft or loss. Plus Device Control to ensure no data may be extracted or accessed unless under strict authorised conditions.

- No fixed Trust equipment, e.g. Desktop PC's, may be moved without the authorisation of the Somerset Partnership NHS Foundation Trust IT Service Desk.

- Protection of IT equipment, including that used off site, is necessary both to reduce the risk of unauthorised access to data and to safeguard against loss or damage.

- All members of staff taking portable PCs, or other hardware or software, off the premises are responsible for their safekeeping. Staff will be expected to specify how long the item is to be offsite. If the arrangement is to be semi-permanent, it should be positively reviewed every quarter. Staff should be made aware of their responsibilities, particularly with regard to data security, and provide assurances that adequate security arrangements will be made.

- Laptop and portable machines should be secured when left unattended. When they are taken off the premises, all efforts must be made to ensure that they are not left unattended in public places. They must be kept out of sight as much as possible when not in use. **On no account should any portable computer equipment be left on view in an unattended car.**

- Portable equipment should be protected at all times from being located in areas vulnerable to opportunist theft e.g. near an open, ground floor window.

A2. Equipment Siting and Protection

- IM&T equipment will always be purchased by, installed and sited in accordance with the manufacturer's specification. Equipment must always be installed by, or with the permission of, the Somerset Partnership NHS Foundation Trust IT Services Department. This includes the attachment of PCs to the network.

- Where appropriate, environmental controls will be installed to protect central or 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.

- Care should be taken when drinking and eating as spillages could damage the equipment in areas housing the equipment.

A3. Power Supplies

- Where appropriate, the Trust will have generator backup to the mains electricity supply and critical computer equipment will be fitted with adequate battery back-up to ensure that it does not fail during switchovers between mains and generator.

A4. Cable Routing

- All cabling, electricity or communications, between buildings will, where possible, be via underground conduit not accessible to unauthorised people. Cabling within buildings will be in conduits if surface mounted; otherwise, within the framework of the buildings.

A5. Equipment Maintenance

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

- All personal computers, terminals, printers and network components will be covered by maintenance agreements with third parties for repair provided it is cost effective. Each case will be judged on its merits. All such repairs will only be made on approval by the IT Services Department.

- Records of all faults or suspected faults will be maintained by the IT Service Desk.

A6. Security of Mobile Devices

All mobile devices issued for staff to use within the Trust will be secured in one of the following ways:-

- Blackberries

    - Handset encryption will be implemented on each device including the encryption of the memory card held in the device. This will be in addition to the security and encryption already implemented as standard on the handset.

    - Devices will be secured through the use of password which is unique to each hand set and known only to the staff member the device is issued to.

- Laptop/Ultra Mobile Note books, etc (Windows Operating System)

    - All devices will be secured through the use of SafeBoot encryption

- iPad/iPhone/Android Tablets

These devices will be secured through the use of Mobile Iron

APPENDIX B

AUTHORISATION FOR SYSTEM ACCESS

Users should refer to the Starters and Leavers procedure for the authorisation of new staff joining the Trust.

B1. Usernames for logging on to the Trust network

- Every member of staff who needs to be able to access the Trust's network to perform their job role must have their own individual logon.
- A request form can be obtained from the Trust Intranet or by contacting the IT Service Desk. The form must be authorised by the person's line manager and sent to the IT Service Desk.
- On submission of an appropriately completed and authorised Request for Network Access form, IT Services will issue each member of staff with a username and a password.
- If a new member of staff will require access to the Trust network on their first working day, their line manager should ensure that the request form is submitted in advance.
- In all cases, staff should allow a minimum of 3 working days for the request to be processed. Where the name of the member of staff is not known until the day that they start work for the Trust e.g. Agency Staff, the form must be completed with all other information and submitted to the IT Service Desk with a note to say that the line manager will contact the IT Service Desk with the remainder of the information on the given start date. Any deviation from the above may result in a delay in the setting up of the username and password.
- The first time the user logs on to the network they will be automatically prompted to change their password.
- The individual staff member is responsible for everything accessed and actioned using their username and password.
- Staff members must not, under any circumstance, share their username and password.
- Where there is a genuine business need to share an e-mail inbox and/or calendar, the IT Service Desk will advise the staff member how this can be achieved whilst maintaining secure practice.

B2. Passwords

- All staff is given access rights and privileges to the various systems in accordance with the area in which they are working and the type of data they require to do their job.

- All staff will have a log-in for the systems that they use. It is unacceptable behaviour for any member of staff to request any other member of staff to log them into the Trust network and systems.

- Any passwords issued to staff are for their use only. Passwords must not be written down or shared with others under any circumstances. It is therefore not acceptable behaviour for any staff member to share their username and password or smartcard with anyone else under any circumstances.

- Staff is personally responsible for anything actioned using their individual username and password.

- To allow another person to access the system under a password that is not their own is a breach of the organisations Security Policy and may potentially result in disciplinary action and/or even Legal action being taken.

- Good practice states:

  - Passwords should be a minimum of 8 characters and, ideally, should be a mixture of letters and numbers, capitals and lower case letters and special characters, such as $%^&*.

  - Names and words that can be found in a dictionary should not be used as these are not sufficiently secure; nor should names of family members, close pets or other easily collected data that may be passed on in general conversation. If a postcode or car registration number is used it must not be a current one as this is also not sufficiently secure.

  - Passwords must be changed on a regular basis. The current Trust policy is for passwords to be changed every 60 days. If your password has not changed within this period then you should contact the IT Service Desk and inform them of this.

- Where it is necessary to access another member of staffs email account e.g.: long term sickness, disciplinary investigation etc., a request must be made to the Director of Finance and Business Development who will arrange for IT to provide access if appropriate.

B3. Smartcards

- Detailed guidance for the use of smartcards is issued to individual users along with their card.

- Smartcard users must keep their cards safe at all times and immediately report the loss of the card or the disclosure of the PIN.

- The PIN should not be written down or disclosed to anyone else under any circumstances.

- Smartcards must only be used by the owner of the card and must not be shared.

B4. When a Member of Staff Leaves the Trust or Changes Role

- It is the responsibility of the line manager concerned to ensure that the IT Service Desk is informed when a member of staff with access to the Trust network leaves or changes their role.

APPENDIX C

DEALING WITH SENSITIVE INFORMATION

Bulk transfer of patient sensitive information to an organisation outside of Somerset Partnership must only be conducted in accordance with the guidelines in Appendix H. The definition of bulk transfer is when more then 51 records of sensitive information requires transferring outside of the Trust.

Sensitive or Patient Identifiable data can only be stored on approved Secure media and locations as approved by the Trust, such as Server shares, approved Secure USB solutions and where absolutely unavoidable mobile computing such as laptops, all these will need to be authorised by the Trust IT Security Manager.

(See definition of Sensitive and Personal Data.)

C1. 'Dos and Don'ts'

The table below sets out what staff should and should not be doing with sensitive information in a clear and concise checklist:

Don't		**Do**	
☒	Don't store sensitive information (patient or other) on removable media (this includes CD ROMs, Memory Sticks, Smart Phones, Personal Data Assistants (PDAs), Laptops, etc)	☑	Do remember you are responsible for all equipment and passwords issued to you.
☒	Don't give out service user or staff personal information unless you definitely know it is permitted and the person asking is allowed to receive it	☑	Do contact your line manager, or Information and Records Officer if in doubt about giving any information out
☒	Don't send information if you think it is insecure	☑	Do ensure you abide by the Trust's safe haven and procedures (Appendix M)
☒	Don't use home IT equipment for work purposes; contact your line manager to see if Trust equipment is available	☑	Do ensure that when you transport equipment or records that you do so securely
☒	Don't allow anyone to know your passwords	☑	Do ensure that all sensitive information is stored securely even when it is in use
☒	Don't send inappropriate e-mails or visit inappropriate websites	☑	Do ensure you ask your line manager if you are unsure
☒	Don't write down your passwords; others can find and use them	☑	Do always lock your computer if leaving it for a short time. Always log off if you are leaving your PC for a longer period.

Don't		Do	
		☑	Do ensure you keep trust equipment secured when not in the office
☒	Don't leave Trust equipment unattended in vehicles	☑	Do always use the word (encrypt) in the subject heading of a Trust email or ensure you use Secure Send, if sending e-mails to anyone other than organisations on the secure list :– • Somerset Partnership e-mail • NHS Somerset • Taunton & Somerset NHS Foundation Trust • Yeovil District Hospital NHS Foundation Trust • Somerset County Council • SWCSU • Somerset CCG

C2. Working with Patient Information

We all have legal responsibilities under the Data Protection Act (1998) and the Computer Misuse Act (1990) to ensure that unauthorised access to our data is prevented and also that our data is accurate and kept up to date.

- All staff must be made aware of their responsibilities under these Acts and must not be allowed access to the Trust's computer systems until Management is satisfied that they understand and agree to these responsibilities.
- It is the policy of the Trust to restrict access to identifiable patient information to those who need to see it.
- Wherever possible, patient information will be fully anonymised, but where this is not possible, the number of data items which could aid identification of any individual will be minimised.
- The Trust will maintain procedures for handling requests for identifiable patient information.
- The Caldicott Guardian will oversee all procedures affecting access to person identifiable health data.

Where identifiable patient information is held, the Data Protection Officer will ensure compliance with the Data Protection Act (1998) and the eight principles there in:

- Principle 1 – 'The information to be contained in personal data shall be obtained, and personal data shall be processed, **fairly and lawfully**..
- Principle 2 – 'Personal data shall be held only for one or more **specified and lawful purposes**.'

- Principle 3 - ‘Personal data held for any purpose, or purposes, shall be **adequate, relevant and not excessive** in relation to that purpose or those purposes.’
- Principle 4 - ‘Personal data shall be **accurate and, where necessary, kept up to date.**’
- Principle 5 - ‘Personal data held for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes.’
- Principle 6 – **Data Subject Access Rights** - ‘An individual shall be entitled, at reasonable intervals and without undue delay or expense,:
    - to be informed by any data user whether he holds personal data of which that individual is the subject;
    - to have access to any such data held by a data user; and
    - where appropriate, to have such data corrected or erased.
- Principle 7 - ‘**Appropriate security measures** shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.’
- Principle 8 – Ensuring Adequate protection for **Overseas Transfers.**

The Data Protection Officer will periodically review the Trust’s compliance with these eight principles.

The IT Security Officer(s) will be responsible for ensuring that all internal IT development projects are undertaken in a controlled and secure manner.

All systems will be password protected.

When any change(s) to systems are required they will be reviewed by the IT Security Officers to ensure there is no impact on security.

C3. Sharing Data/Information with Partner Organisations

The Trust works with partner organisations that have a legitimate role to play in delivering care to NHS patients. Partners, in this context, are taken to be:

- Social Services
- Education Services
- Voluntary Sector Providers
- Private Sector Providers
- District Councils

The organisation will ensure that secure methods of transferring information exist and that Information Sharing Protocols are in place prior to the passing of any information.

Currently all transmissions of information via e-mail must be encrypted using the word **(encrypt)**, (this must be the word encrypt enclosed in round brackets), **in the subject heading** of a Somerset Partnership email or information must be sent via Secure Send, with the exception of:-

- Somerset Partnership email
- Somerset CCG
- Taunton & Somerset NHS Foundation Trust

- Yeovil District Hospital NHS Foundation Trust
- Somerset County Council

These highlighted sites are secured and do not require encryption. Using (encrypt) also ensures that attachments are securely transmitted.

If you are in any doubt it is better to add (encrypt) to the subject line as if it is not needed the system will ignore the instruction.

C4. Sharing Data/Information with non-partner Organisations

All such requests must be passed to the Records and Information Governance Manager for action.

The Trust from time to time receives requests for person-identifiable information. Organisations requesting such information include:

- The Police.
- Insurance companies.
- Solicitors.

Whilst such requests may be legitimate, the Trust will ensure the use of such information is not abused, by applying the following principles when considering the release of the information to non-NHS organisations:

- Information will not be released without the written consent of the individual concerned.
- Individuals will be fully informed that information is being released and of the purpose(s) for which it is being used.
- Individuals will be given the right to review the information being released and given the opportunity to correct or otherwise amend such information before release.

These requirements may be waived in certain conditions e.g. as a result of a court order, but only after the Caldicott Guardian has obtained authorisation.

APPENDIX D

INSTALLATION AND SECURITY OF SOFTWARE APPLICATIONS

D1. Software Licensing

- All new patch releases or updates are fully tested before live implementation to ensure no business impact to the Trust.
- An agreed maximum period of time before release of updates and implementation is no more than 10 working days.
- The Trust has a legal responsibility and IT Services has a contractual obligation to ensure that there are sufficient licenses for all instances of a particular piece of software in use within the Trust.
- As such IT Services will maintain monitoring systems to ensure that all proprietary software products on PCs and Servers are used legally.
- If there needs to be more than one instance of a piece of particular piece of software, then either multiple licenses or a license covering multiple users will be purchased.

D2. Virus Protection provided by the Trust

- IT Services and The Trust will provide a suitable software solution for virus checking. Responsibility for making sure that the software is up to date lies with the IT Services Team.
- IT equipment permanently attached to the network will be automatically updated as new versions become available.
- For equipment not permanently attached to the network, updates are configured to automatically download and prompt the user for installation, the user should allow these updates to install at their convenience and not disable any Trust setup auto updates. Updates will also be triggered once the device is reconnected to the Trust network or via the Trust Virtual Private Network remote working solution, however devices absent from the network in excess of 60 days will be disabled and require IT support to re-enable.
- To minimise the risk of viral or malware infection, staff must not under any circumstances connect unauthorised or portable media or equipment to the Trusts network without first seeking advice from the IT Services.

D3. Installation of Authorised Software

- Authorised software must be installed by a member of IT or their designated representative. Any business software installed by anyone other than authorised personnel will not be supported by IT Service Desk and may be subject to removal as part of a regular audit cycle.
- If there is a legitimate business need for additional software, the senior manager of the department must make a case for acquiring the software. Consideration must be given to the number of users requiring the software, the training required for the efficient and effective use of the software, and how the software will be supported and maintained. The software will not be adopted as Authorised Software for the Trust without explicit acceptance by the Trust.

- Remove local Administrator rights were possible to reduce the risk of unlicensed software and potential harmful software being loaded.

D4. Installation of Unauthorised Software

- Unauthorised software includes, but is not limited to, games software, non-standard screensavers and wallpaper backgrounds.
- Under no circumstances should unauthorised software be loaded on to Trust equipment. It is a disciplinary offence to copy unauthorised software and may lead to prosecution for theft. This includes the downloading and use of legitimate software termed “Administrator Utilities” or “System Support tools” which gives a member of staff access to areas of the system they would not normally access or be authorised to use.

APPENDIX E

USE OF TRUST EQUIPMENT AND PORTABLE DEVICES

Please see the definitions of Sensitive and Personal Data and Portable Media.

E1. Using Personal IT Equipment for Trust Purposes

- It is not permissible to use personal IT equipment for Trust business purposes, whether this be home desktops or laptops, Personal Digital Assistants, Smart Phones or any other electronic device. The only exception to this is through a Trust approved BYOD (Bring You Own Device) service. *No such service exists at the time of the creation of this Policy.*
- Limited personal use of Trust IT equipment is permissible, eg: small documents, use of internet sites, however staff should not store documents/images which take up a large amount of bandwidth which will have a detrimental effect on Trusts systems. If unsure staff should contact the IT Service desk.
- It is not permissible to connect personal IT equipment to Trust networks or devices, whether this be home desktops or laptops, Personal Digital Assistants, Smart Phones or any other electronic device.
- This policy applies to all electronic equipment including Multi-function devices. Where these devices reach the end of their life and are disposed of, any media used as a temporary store for Trust information must be securely disposed of through secure deletion or destruction via the Trusts Disposal of IT equipment Policy.
- **All** IT equipment within the Trust whether desktops or Laptops are encrypted.

E2. Mobile Devices

The following mobile devices are currently being assessed for their suitability for use within the organisation. Due to the relative costs and functionality of each device it is necessary to "target" these devices at the most appropriate staff group suited to each device.

Currently in use

Blackberry Handsets – Staff Group - Service managers and above

- Access to emails and calendar whilst on the move.

Under evaluation

iPad Tablets – Staff Group – Under review /Evaluation

(Due to the relative costs of these devices it is likely that their use will be restricted to Executive and non-Executive Board Members only. This will help to significantly reduce the volume of paper required to be transported by this staff group).

- Access to emails and calendar whilst on the move.
- Board Papers distribution.
- Meeting papers distribution.

iPhone – Staff Group – Under review /Evaluation

- Access to emails and calendar whilst on the move.
- Limited access to RiO for outcoming and progress note recording – Functionality not currently available.

Andriod Tablets – Staff Group – Under review /Evaluation

- Access to emails and calendar whilst on the move.
- Limited access to RiO for outcoming and progress note recording – Functionality not currently available.

E3. Removable Media

A user should not use any memory stick unless allocated one by the Trust. The memory sticks used by the organisation are encrypted. If a Memory Stick has been allocated by the Trust then it must only be used for Trust-related work.

By accepting a Trust memory stick, the user is agreeing that:

- Only secured and approved memory sticks may be used to store Trust data for Trust business, all other memory sticks will be disabled from storing Trust data, where practical.
- the memory stick will not be used in non-Partnership IT equipment, including home equipment or other non-Partnership NHS equipment. The only exception to this is for educational purpose, for the transfer of coursework or credits evidence.
- they will not copy information onto non-approved systems/storage devices regardless of reason.
- data stored on the stick will always be encrypted and that data stored will be removed at the earliest possible time to ensure accidental loss does not occur.
- when leaving the employ of the Trust, the data stick will be returned along with other equipment allocated to the user.

It is the responsibility of all staff to protect the Trust's computer systems from viruses. All media from outside the Trust must be checked for viruses before being used on a Trust machine by first seeking advice from IT Services.

Portable media includes floppy disks, CDs, DVDs, USB keys/memory sticks and all other methods of storing and moving data in an electronic format.

If necessary, and on request, the IT Service Desk will provide guidance on how to virus check media on a Trust PC.

It is not permissible to run programs from USB keys/memory sticks as doing so may present a risk to the network.

Any Portable Media (Trust-owned) device that is used is to be encrypted to the appropriate level before use.

Any loss of portable media must be reported via the Datix system.

APPENDIX F

NETWORK SHARES

F1. Use of the local hard drive, e.g. C drive

- Person-identifiable or commercially sensitive information will not be stored on the local hard drive e.g. C drive, unless authorised by the IT Services team, the data if approved will be secured accordingly and placed in a structure that allows upload to the servers once the device is back on the network so ensuring data backups are achieved, security is maintained and mobile computing is achieved where required by the business.

F2. When Connected to the Trust Network

- Any document saved to the Trust network e.g. a folder on F drive, is automatically backed up as part of the Trust Back-Up and Disaster Recovery Strategy.
- IT Service Desk can be contacted for further information on mapped drives and how to access them.

F3. When Disconnected from the Trust Network

- It is important to note that C drives and other portable media are more prone to corruption than the larger media storage drives such as those maintained by IT Services. In cases where the only copy of a document is on a corrupted drive, IT Services will endeavour to retrieve the document on a Best Efforts basis, but cannot be held responsible for loss of the data if retrieval is not possible.
- It is the responsibility of all staff to ensure important documents are copied onto network drives/shares to protect against data loss.

APPENDIX G

EMAIL AND INTERNAL USAGE

G1. Email and Security

- the email and web-browsing system are provided for authorised business use.
- no patient identifiable information, confidential material or government classified information must be transmitted via email, unless through a secure mechanism, ie via NHSnet email to NHSnet email or using encryption (see Appendix C, section C3).
- Reasonable personal use of the email and web-browsing systems is permissible, in an individual's own time, provided this does not interfere with the performance of work duties.
- internet mail (eg Hotmail, Gmail or Netscape, etc) is not secure and users must consider such email and other information to be public information.

Staff should note that they must not keep emails in their Deleted Items folder. The Trust will be implementing a policy which will automatically delete emails from users Deleted Items folder. These emails will not be recoverable.

It is essential that all information obtained, stored or provided by way of the Trust's email system be dealt with in a secure manner. Accordingly:

- you should password protect your email account and keep your password secret. You agree that you will change it on a regular basis.
- do not disclose your password to another person, or attempt to use the password of another person to access information to which you are not authorised.
- do not permit another person to access and use your email address unless you are authorised to do so by your line manager.
- do not access the email address of another person unless you are authorised to do so.
- you are responsible for the content of all emails sent in your name and you should close your email account when you are not present at the computer.
- staff should familiarise themselves with the current IM&T Security Policy.
- it is advisable to contact the IT Service Desk before opening email attachments when received from an unknown source.
- do not send anything by email that you would not send by letter or fax.
- remember that emails sent abroad may be subject to different laws and information enclosed in them may be subject to export restrictions.
- if you are unsure whether you should send an email please contact your Line Manager or Data Protection Officer before sending it.

G2. Email and Internet usage

E-mails and web-browsing may be monitored for the following purposes.

- to provide details and evidence of business transactions;
- to ensure business procedures are being properly complied with;
- to carry out training and monitoring of service standards;
- to prevent or detect the unauthorised use of communications systems;
- to prevent or detect criminal activities;
- to maintain the effective operation of communications systems.
- Somerset Partnership IT services reserve the right to globally ban, without warning, access to any site deemed inappropriate.

The Trust reserves the right to instigate the monitoring of email and internet usage in the interests of its business needs and to access staff email boxes without the knowledge or permission of individual staff members.

Disciplinary procedures may be instigated if evidence demonstrates that any of the following has taken place:

- transmission of messages containing defamatory material.
- transmission of pornographic or obscene material.
- willfully accessing another user's e-mail to read, send or delete messages without permission.
- knowingly connecting to a site that contains libelous, racially offensive, gambling, obscene, pornographic or sexually explicit material, or is otherwise illegal or offensive.
- introducing a virus into Trust computer systems.
- downloading and installing applications from the Internet without prior consent from the IT Service Desk, regardless of the reasons.
- subscribing to any product or service on the Internet, including news groups and chat rooms which are not work related
- send emails that are, or may be considered to be, abusive, indecent, obscene, rude, sexist, racist, defamatory, or generally distasteful
- do anything which could damage the name and/or reputation of the Trust
- encourage or promote any activities that are, or may be, unlawful or illegal
- encourage or promote activities that are unproductive use of paid time
- act outside of their personal responsibilities within the Trust
- enter into a contractual commitment on behalf of the Trust unless expressly authorised to do so. Staff must comply with all normal policies and procedures of the Trust in this regard.

G3. Email Usage General Principles

Do not auto forward via rules emails to non-Somerset Partnership NHS Foundation Trust email accounts as this can result in security breaches of confidential information entering unsecured email systems.

Attachments that have been received from an external source should be treated with extreme caution, especially those that are unsolicited. Before opening an unsolicited attachment, the receiver should check with the sender concerning the nature and purpose of the attachment.

Viruses and other malicious software are often sent as attachments. For this reason, some attachments may be quarantined to ensure the safety and security of the Trust network (e.g. zipped files and database files) via the Borderware emails which staff must action appropriately. If an individual user needs to receive any file type which may be blocked, the IT Service Desk will advise on the best way of doing this whilst maintaining security of the network.

Where an email is sent with an attachment ensure that the attachment and email are stored within your normal file structure. Email is not designed to hold large numbers of emails with attachments and this can lead to a significant reduction in the performance of the system. Email Boxes are therefore limited to 360mb per user.

G4. Personal Use of Email

It is permissible for staff to send and receive email during breaks for incidental personal purposes provided that doing so does not involve a substantial expenditure of time, or is used for profit.

The circulation of non-business emails should be avoided as rapid distribution across the Trust can place unnecessary pressure on the Trust email systems, exposing trusts systems to potential viruses and malware.

The Trust has the final decision on deciding what constitutes inappropriate use. All suspected infringements will be considered on a case by case basis.

G5. Social Networking Sites and Media

Whilst at work

The use of Social Networking Sites is restricted.

- Unless specifically authorised to do so, staff should not access social networking sites from Trust computers or within Trust time.

- All social networking sites have access controls placed upon them via IT Services.

Outside of work

The Trust recognises that social networking sites are increasingly useful communication tools and acknowledges the right of staff to freedom of expression in their personal lives. However, it is critical that members of staff are aware of the legal and organisational requirements for responsible use of this media and the potential implications on their employment of misuse of this media.

The Standards of Personal Conduct sets out the Trust's expectation for the conduct of members of staff and whilst the Trust has no control over staff and how they use social media in there own time, there have been a number of incidents where staff have posted information on their own pages of social networking sites, and this information has become known to service users.

Staff should therefore bear in mind the following guidelines when using these sites:-

- Keep your personal and professional life as separate as far as possible. Be aware that your conduct online could still jeopardise your professional registration if it calls your fitness to practise into question.
- Staff should be mindful of their own professional codes of conduct and guidance on confidentiality where these apply, also **you have contractual duties to observe patient confidentiality and to keep confidential Trust information**.
- Staff should consider very carefully when they grant access to their social networking pages in terms of content and information. Under no circumstances should patient identifiable information be posted on social network sites.
- Do not use social networks to build or pursue relationships with patients and service users, even if they are no longer in your care. Do not accept friendship requests from current or former patients.
- Do not discuss work-related issues online, including conversations about patients or complaints about colleagues. Even when anonymised, these are likely to be inappropriate. Do not use social networking sites to bully or intimidate colleagues.
- Do not post pictures of patients or service users, even if they ask you to do this. Do not use your mobile phone camera in the workplace.
- Social networking sites should not be used for raising and escalating concerns, if you have concerns and feel unable to raise these with you line manager, please use the Trusts Whistle Blowing policy procedures.
- Where staff grant access to their social networking site they need to be aware of the possibility of this information being viewed, and that this might possibly place them in a situation where their own privacy/security might be at risk. Information posted online is public, it can be copied and redistributed. Presume that everything you post online will be permanent and will be shared.
- Staff should consider the potential risk of posting family photographs or details of other family members on the website.
- Staff should consult the social networking site provider and their guidance on possible safeguards and access settings to their personal information.

Please note that failure to comply with these requirements may be considered as misconduct as defined in the Trust's Disciplinary Procedure and will the dealt with in accordance with these procedures.

Exemptions for Social Media use

Some services are wishing to stay connected to their clients through the use of Social Media. Where a service wishes to utilise this type of communication with Service Users or Carers, then the following process must be followed:-

1. A request in writing **must** be made to the Director of Finance and Business Development for the Trusts ICT Business Group to review.
2. The Trusts ICT Business Group will review the request and if found to be valid discuss the necessary changes required to infrastructure in order to support the request.

3. The request will be passed to the Information Governance and Caldicott Group with the recommendation of the ICT Group and details of the Infrastructure changes.

It should be noted that the ICT business group meets on a monthly basis and the Information Governance and Caldicott Group meets quarterly.

G6. Email Etiquette

As with any other form of communication, what & how an email message is constructed can have an impact on the information being shared. The following guidelines can help your messages to be effective.

Ask yourself the following questions

- **Why ?** - am I sending this email, could it be done via another method, telephone, face to face meeting, etc?
- **Who ?** – am I sending this email to - think of all the emails you receive each day which are copied to you for information, are you therefore copying in people for the right reasons?
- **What ?** – are you sending. Is the attachment available to the target audience via an alternative medium or already exists in an area they have access to? If so then email them telling them where to find it. Is the email time limited and therefore should you be putting an expiry time on the email so it is auto deleted after x days?

Important considerations

- email contents should be carefully considered before despatch. What one person may finds inoffensive, others may not.
- inappropriate content in emails sent by, or in the name of, a member of staff may lead to legal proceedings against the sender and/or the Trust, in the same way as inappropriate content in a fax, letter or verbal statement.
- email messages may have to be disclosed in court proceedings or as part of an investigation by a regulatory body, no matter how confidential or private they may be.
- look at the email and think how you would feel if you received it. Remember the receiver cannot defend himself or herself immediately.
- do not cc: people who have no direct involvement. Think how long it takes you to go through your emails and how many you receive that only require you to read and delete.
- do NOT SHOUT at people using CAPITALS or punctuation!!!!!!!!. Anger should not be conveyed this way. It is likely to be more appropriate to speak to the person concerned on the telephone, or arrange a meeting.
- email should be treated in the same manner as a memo or short letter; it is not a replacement for meetings or telephone calls.
- if the matter to be discussed requires more than three people to liaise with each other, a meeting should be called. After the meeting, email can be used to send updates or notes to each other. However, if a meeting is not possible, make sure that the email is clear on the objectives and responsibilities of the individuals concerned.

- if the subject is very sensitive, it might be better to telephone or arrange a meeting to allow immediate feedback (remember that emails are subject to the same legal restrictions as written material).
- if the subject is confidential, then mark the email accordingly.
- take care how you address your email. Care should also be taken when using the 'reply' and 'reply to all' functions. Careless use of these functions can lead to emails being sent to inappropriate recipients, and may cause a breach of confidentiality.
- remember emails can bind parties to contractual obligations in the same way as paper documents. You should take the same care in drafting and sending emails as you would for any other written communication.
- you should check your email before it is sent just as you would a letter
- when using internal email, the 'return receipt' function can be used to confirm delivery. A receipt is not a guarantee that the email has been read in full, however, and in some cases the option may not work. .
- do not send emails inviting people to attend meetings at short notice. Allow reasonable time for them to open and read their emails.
- if actions need to take place arising from the email, list them and identify who is to be responsible for them. Do not assume that people will pick up their tasks just from the general contents of the email.
- **delete obsolete emails**. Archive email that you need to retain but do not need to refer to on a regular basis (in accordance with the retention policy). Remember to empty the 'recycle bin' regularly.
- when you are not available you should use the 'out of office' facility. Failure to use this could result in emails not being opened in your absence and the sender not being aware that you are not available to respond. The auto reply should read "**I am out of the office until** (enter the date you will return to work) **when I will read and respond to your email. In my absence please contact** (enter contact name and number of a colleague who can be contacted in your absence)." It is not advisable to state that you are on holiday as this implies that your home may be unoccupied
- do not print all email messages as this wastes paper.
- if you use the personal address book on your computer remember to keep it up to date.
- when sending personal emails, indicate this by using the subject header 'Personal'

G7. Junk Email

Email should not be sent to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many users ("spamming") is wasteful of user time and can disrupt the service for other users.

G8. Computer Virus Protection

Email is the most common method of transmitting computer viruses. For this reason it is essential for your security, and for the security of other NHS messaging service users, that all files brought onto your system from email, disk or other sources are scanned by up to date, reputable anti-virus software.

- Do not open attachments from an unknown source.
- Beware of unexpected messages with attachments even from a known source.
- Where you are aware of infection on your system do not send further email until the infection is cleared. Seek advice from the Somerset Partnership IT Service Desk.
- Make appropriate use of borderware to block and screen suspect emails.

G9. Data Protection Act 1998

The provisions of the Data Protection Act 1998 apply to information about living individuals (personal data) contained in any correspondence; including emails Personal data covered by the 1998 Act includes facts, intentions and opinions about individuals. Staff should refer to the Trust's Data Protection Statement for full details of the implications of the Act. If you are unsure of any aspect of email security, please contact the IT Service Desk.

If you are not sure how to undertake any of the above functions contact the IT Service Desk to request training.

G10. Copyright and Intellectual Property Rights

Email is subject to the same restrictions as written material in books, magazines or other paper materials with respect to copyright and intellectual property rights. You must seek permission from the relevant parties with respect to the use in any way of material not owned by the Trust.

G11. Web Browsing Guidelines

Access to the Internet is through the secure gateway provided through NHSnet. This gateway allows outbound Internet access only, thus securing all NHSnet connected sites from probing attacks from external Internet users.

The Trust also has its own security firewall, which provides an additional level of protection. The Internet link is provided for health authority authorised business. Reasonable personal use is permitted in an individual's own time provided this does not interfere with the performance of work duties. A line manager can limit personal access to the Internet and staff must act in accordance with their line manager's guidelines. The Trust has the final decision on deciding what constitutes excessive use. The Trust takes no direct responsibility for the actions of any individual with regard to the misuse of the Internet.

The Trust has deemed it to be a disciplinary offence for staff to knowingly:

- connect to any site that contains libelous, racially offensive, gambling, obscene, pornographic or sexually explicit material, or is otherwise illegal or offensive.
- introduce a virus into Trust computer systems.
- download and install applications from the Internet without prior consent from the IT Service Desk
- subscribe to any product or service on the Internet, including news groups and chat rooms which are not work related.

The Trust reserves the right, consistent with UK law, to monitor all Internet access. No member of staff should consider information sent/received through the Internet as his/her private information.

The use of the Internet is a privilege, not a right. Inappropriate use, including any violation of this policy, may result in the withdrawal of the facility, disciplinary action (including possible termination of contract) and/or notification to the proper authorities for criminal/civil proceedings, depending upon the violation.

APPENDIX H

BULK TRANSFER OF INFORMATION

1. EXPLANATION OF TERMS USED

Bulk transfers	More than 51 records being transferred together at one time.
Sensitive data	Data Protection Definition – In this Act 'sensitive personal data' means personal data consisting of information as to: (a) the racial or ethnic origin of the data subject; (b) their political opinions; (c) their religious beliefs or other beliefs of a similar nature; (d) their membership of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992; (e) their physical or mental health condition; (f) their sexual life; (g) the commission or alleged commission by them of any offence; (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

2. BULK TRANSFERS

- All bulk **electronic** transfers of sensitive data shall be made by the Information Department, and authorised by the Director of Finance and Business Development.
- All other bulk transfers of sensitive data via non-electronic means must be approved by the Information Governance and Records Manager, this include medical records, etc.
- In the event of a bulk transfer of electronic information being required, the staff member should contact the Director of Finance and Business Development or, if unavailable, the Head of Information
- The information for transferral will be reviewed (by the staff member and either the Director of Finance, Head of Information or Information Governance and Records Manager) and, where appropriate, information may be removed (where no added benefit to the third party exists).
- A view will be taken on whether the transfer can be performed by the requester (with Information Department support) or whether the Head of Information or clinical staff will need to make the transfer.

- There several methods of electronic transferal:-

  a) Sending the information from one NHS.net email address to NHS.net email **only** (this utilises the NHS Infrastructure)

  b) Sending an email with the word (encrypt) in the subject heading. This will force the email to be encrypted to the correct NHS Standard and any recipient not considered secured.

  c) Transferring the data via a secured website (usually identified by accessing the site via HTTPs)

  If none of these options are available, it will be at the discretion of the Director of Finance and Business Development as to whether the transfer will go ahead (using the most secure transfer mechanism available).

- **Trust Staff transporting patient records**

  It is vitally important that patients as members of the public feel their sensitive and personal information is kept safe and secure when being transported.

  The **minimum of patient records** must be transported **at any one time** so that loss of this information is minimised.

  No bulk transfer (50 record sets) of patient **electronic information** can take place unless approved by the Trust's SIRO.

  Transporting of Patient, Staff or Corporate Sensitive Records is described in more detail within the Record Keeping and Records Management Policy.

- **Third Party Organisations**

  Where staff work out of offices of third party organisations and using the third parties IT equipment for the storage of information and data, then the third party is the Data Owner of the information and data held on the systems, (example : District Nurse working out of a GP Practice). Therefore no bulk transfers of information can be carried out from the third party organisation without the authorisation of the third parties Caldicott guardian or equivalent, and agreement with the Partnerships Caldicott guardian. Staff wanting to carry out these types of transfers should contact the Trusts Information Team for further advice.

APPENDIX I

DATA QUALITY

1.1 Although there are many aspects of good quality data, the key indicators are:

- **Validity.** All data held on Trust computer systems must be valid. Where codes are used, these comply with national standards or map to national values. Wherever possible, all systems will only accept valid entries through application validation and rules.
- **Completeness.** All mandatory data items within a data set (defined by Connecting for Health or other standard-defining organisations) will be completed, wherever possible, through the use of the appropriate standard definition. Default codes will not be used as a substitute for real data.
- **Consistency.** Data items should be internally consistent and within the context to which they have been defined.
- **Coverage.** Data will reflect all the work done by the Trust. In terms of EPR Systems, inpatient, outpatient and community activity, and certain procedures, should all be recorded. Correct procedures are essential to ensure complete data capture.
- **Accuracy.** Data recorded in notes and on computer systems must accurately reflect what actually happened. All reference tables, such as GPs and postcodes, will be updated regularly. This will be within a month of publication unless there are serious doubts about the quality of the data supplied. Every opportunity should be taken to check demographic details, including equality information relating to ethnicity, age, gender and first language for both patients and staff. Inaccurate demographics may result in important communications being mislaid or incorrect identification.
- **Timeliness.** The recording of all information should conform to the Clinical Record Keeping Policy. Recording of timely information is beneficial to the care and treatment of the patient. All data will be recorded within timescales set, which will enable that data to be included in scheduled national returns. The accurate recording of data items must not, however, be allowed to delay urgent patient treatment.

1.2 **Documented Procedures**

- Careful monitoring and error correction supports good quality data, but it is more effective and efficient for data to be entered correctly the first time. In order to achieve this, ward/team managers must establish robust procedures for staff to be trained and supported in their work.
- Any changes which require alteration following the identification of a data quality issue will be documented (including the minutes of the meetings where the issues have been actioned). This will include the process to be used by the relevant Information Asset Owner or Information Asset Owner Administrator to rectify any data quality issues. Where agreement exists for on-going data quality issues to be addressed, (by a routine process) this is documented and performed until a permanent solution has been found to the problem within the relevant application.

1.3 Identifying and Correcting Errors

Errors should be identified as close to the point of entry as possible. Methods by which this can be achieved are:

- the use of routine reports to highlight areas of poor data quality. Where appropriate this will be rectified either by the relevant Information Asset Owner or Asset Owner Administrator.
- a programme of weekly and monthly error reports should be produced by the relevant Information Asset Owner or Asset Owner Administrator and actioned where appropriate.
- the use of external data sources to further support and identify data quality issues.
- regarding the Trust's EPR, many errors can be corrected by users; see Appendix A for further details.
- any other errors should be reported to the IT Service Desk on 0300 3230111 who will then pass the details of the issue onto the Somerset Partnership Information Delivery Team who will rectify the issue, after discussion with the clinician involved where appropriate.

If any individual believes that information has been entered into a system incorrectly then they should contact the IT Service Desk for further advice and guidance. They will be able to provide advice on what information can be changed by the end user and what requires escalation to the Application Support Team.

1.4 Conformance of Systems to NHS Data Dictionary Standards

All of the systems in use by the Trust will whenever possible comply with the NHS Data Dictionary and associated standards. Where systems comply with these definitions data quality should be less of a problem to the organisation providing that processes are in place to ensure that these definitions and standards cannot be switched off or disabled.
Currently the only systems in use by the Trust which conform to these standards are as follows:-

- RiO – SUS data flows, NDTMS data flows, MHMDS data flows
- Cerner – SUS data flows
- HP Swift – SUS data flows
- Blithe Lillie – Sexual Health data flows

It should be noted that both the Cerner and HP Swift systems are managed and maintained by two acute hospitals and as such the Trust has no control over compliance to the NHS Data Dictionary or whether functionality is switched off.

Where systems submit data directly to SUS, the Trust will ensure that these files are validated against Information Governance Requirement 507 so that all files submitted are validated on a monthly basis and meet a minimum of Level 2 standard.

1.5 Measurement and Improvement of Good Data Quality

Data quality will be subject to control processes within the Trust and will also be subject to external scrutiny.

Internally

- **Clinical Focus.** The use of reports within systems, and provided centrally, to support clinicians in good data quality management and clinical care.
- **Clinical Systems Information Management .** The Information Team will take responsibility for the monitoring of data quality with regard to the Trust's EPR systems, with issues being discussed on a weekly basis at the Information Team meeting. An Action Plan will be maintained by this department and will be provided on a quarterly basis as the Data Quality Action Plan to the Caldicott and Information Governance Group for review. The tools used should include reports written from Trust data sources, which review known problems to ensure monitoring and, where appropriate, reports should be written to include new areas.
- The Information Team will also be responsible for reviewing Information Standard Bulletins from the NHS Information Centre to review and assess their impact on clinical systems.
- Various data sources are used to review data quality based on National Guidance for data completeness in the following areas: Information Governance; SUS Data Quality Dashboard and eDQRS; MHMDS Data Completeness and current PCT Contract requirements eg coding completeness, NHS numbers, ethnic group and outpatient outcomes. Internal monitoring reports will be used to inform management, improve processes, identify training needs and amend documentation.
- **Senior Management Operational Group.** Information about the service is provided via the Trust's Balanced Score Card system to ensure monitoring and to improve the service. This group consists of Service Managers and Operational Directors who will raise, where required, queries over data quality when they believe the information to be inaccurate with the Performance Manager for review and action.
- **Clinical Governance.** The use of reports within systems and provided centrally to support the Quality Improvement Plan process for central and decentralised clinical audit.
- **Operational Managers** (Service Managers / Team Managers / Unit Managers). Reports are provided to this group of staff for them to review activity with regard to their areas of responsibility. By providing activity reports to this group, they are able to review the activity by comparison to other "like" areas.

Externally

- The Trust will use external data sources to review its own information, highlighting areas of poor data quality for action within the Trust.
- The Trust will aim to be significantly above average in all indicators and will strive for 100% accuracy. The Trust will act on all enquiries and complaints from all users or providers of data.

APPENDIX J

PROCUREMENT

When procuring equipment for operational use:

- All Trust IT equipment should be purchased in conjunction with the Trust's procurement procedure via the IT Department and in accordance with the Trust's Standing Financial Instructions. Failure to comply with this may result in the equipment not being supported by IT.
- Where a laptop is issued to a member of staff, they will not be given a desktop PC; instead, they will be provided with a docking station to enable the laptop to function as a desktop when they are at their designated base.

Procurement procedures should encompass all Information Governance issues with regard to security, Privacy Impact Assessments and, where a clinical impact exists, they should be assessed by the Clinical Risk Officer. All these issues should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for any IT-based system.

All hardware and software procurements should ensure that:

- hardware or software changes which may affect network management are agreed by all the parties affected;
- any new IT facilities provide an appropriate level of security and will not adversely affect existing security;
- mandatory and desirable security requirements are included in procurement specifications by the IT Security Officer and/or Director of Finance and Business Development and they are consulted to ensure that the selected hardware or software will meet the agreed security requirement and be supported by IT Services.
- the procurement process should take into account the need for hardware and software compatibility to support the installation's contingency and recovery arrangements.
- project approval will be withheld until the necessary security requirements have been built into the project plan.
- all procurements should be run in conjunction with IT Services along with appropriate Project Management support.
- there should be formal documented user acceptance criteria against which the system can be tested. These criteria should specifically cover Information Governance requirements that should be approved by the IT Security Officer and Director of Finance and Business Development as part of the handover process.
- any system procured should consist of at least 2 versions:
    - a live system for operational use
    - a non-live system (test) to carry out testing of new software releases or evaluate software problems without impact on operational systems.

APPENDIX K

LEGAL FRAMEWORK FOR INFORMATION SECURITY POLICY:

Data Protection Act 1998 – refer to Data Protection, Caldicott and Confidentiality Policy for
details.

The Calicott Principles - refer to Data Protection, Caldicott and Confidentiality Policy for details.

Criminal Justice Act 2008

The Criminal Justice Act 2008 provided enhanced powers to the Information Commissioner; bodies or individuals who are aware of information risks but have not taken reasonable and appropriate steps to mitigate against them can be liable to fines of up to £500,000. These provisions place a direct responsibility on HPCT and its entire staff at every level to adopt and maintain good
Information security practices.

Common law of confidentiality

Health information is collected from patients in confidence and attracts a legal duty of confidence until it has been effectively anonymised. This legal duty (established under common law) prohibits information use and disclosure without consent - effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is robust public interest justification.

Human Rights Act 1998

Citizens who believe their rights have been unreasonably interfered with can bring Human Rights cases in UK courts. The principles of data protection are echoed in Article 8 of the European Convention on Human Rights.

Freedom of Information Act 2000

This Act is enforced by the Information Commissioner. - refer to the Freedom of Information Policy.

Computer Misuse Act 1990

The Computer Misuse Act 1990 is used in the prosecution of people who deliberately gain access
to and potentially modify computer data to which they aren't authorised. The main considerations for employees are that they should ensure that they are authorised to access the systems and that they report any attempts by others to gain unauthorised access to the Information Governance Manager and as an incident on the Safeguard System.

Three key offences:

- Unauthorised access to computer material would cover hacking into systems and taking information; falsifying records

- Unauthorised access with criminal intent to commit or facilitate the commission of other offences - would cover hacking with the intent to commit fraud with the information.
- Unauthorised intentional modification of material e.g. viruses.

Copyright Designs and Patents Act (1988)

Copying e.g. software, publications, photos etc must only be undertaken with the written authority of the copyright holder. The Trust will ensure that all staff comply with the law on licensed products. Appropriate software products will be used to monitor this. All users will ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software, publications etc and offenders are also liable to disciplinary action.
This also includes the trading in Intellectual Property – copyright, designs, patents and trademarks.

Health and Safety at Work Act 1974 (Computers)

Employees must take reasonable care of their work place. If you are not sure about health and safety procedures then you should contact your line manager. Make sure that the working practices of your department allow the safe and healthy use of computer equipment. Information for computer users is available from the Occupational Health Department.

British Standard BS7799
This is a code of practice for managing the information security within an organisation. The Security Policy document is intended to comply with the framework of this standard. This has been adopted as an international standard (ISO 17799).

APPENDIX L

REMOTE WORKING

Remotely accessing site-based computer systems extends the flexibility of NHS services, allowing staff to work from home or on the move, known as mobile working. The demand for both is increasing and will continue to increase as technology develops and work practices change.

This Appendix provides guidelines to ensure that all Trust staff working away from their base comply with NHS IT Security, Confidentiality and Health & Safety requirements and enable the management of the associated risks effectively.

This Appendix identifies the IT-related risks, costs and future developments and the responsibilities of organisations and of remote workers and the IT Department.

L1. Overview

This Policy is for all Somerset Partnership staff and other individuals authorised to use Trust IT systems and relates to IT issues only. It covers all types of remote access via IT equipment whether fixed or 'roving' including:

- Mobile users (eg Community Nurses, Managers)
- Home workers
- Remote Office workers

This policy, covering all types of remote access via IT equipment, explains the principles, responsibilities and expectations of staff to ensure a secure, reliable IT service for all. It details the risks to Somerset Partnership of providing a remote access service to workers, as well as the benefits.

The policy also specifies the options, Broadband and 3G, which are available for remotely accessing Somerset NHS sites.

In addition, the Addendum provide detailed information on other aspects associated with remote working:

- Mobile working code of conduct
- Risk Details

L2 Duties and Responsibilities

L2.1 All Staff

The Trust must ensure that everyone who accesses NHS systems away from their base site is aware of the Remote Access Appendix contained within this Policy and that they understand their responsibility to protect both patient and business confidentiality.

L2.2 Remote Access User Must:

- Adhere to the code of conduct detailed in Addendum (i).
- Comply with the Information Security Policy and associated standards.

- Only access Trust systems using methods defined and approved by the IT Department
- Safeguard NHS equipment and information resources.
- Take great care around use and storage of USB memory sticks, which should only be used for sensitive information when no other option exists.
- Ensure they only access systems and information to which they are entitled.
- Notify the IT service Desk immediately of any security incidents and breaches.
- Return all relevant equipment to IT Department when it is no longer required, when leaving the Trust or in the event of an equipment failure.

L2.3 Managers will:

- Have overall responsibility to ensure the remote access user abides by all the applicable policies and standards.
- For each remote access application, use Appendix C to assess risks and identify controls needed to reduce risks to an acceptable level.
- Provide written authorisation for all remote access users and detail the level of access required.
- Clearly define to the remote access user their responsibilities as a remote user of systems.
- Regularly review, at least every six months, the list of authorised remote access users for their area, to confirm that there is still a valid requirement.
- Inform the IT Service Desk immediately when authorisation for remote access is no longer required.
- Ensure remote access requirements are appropriate to business need.
- Notify the IT Service Desk of any security incidents and breaches.

L2.4 IT System Administrator will:

- Restrict the remote user's access to the minimum services and function necessary for the required process.
- Regularly review (at least every six months) the list of authorised remote access users and remote access logs to confirm that there is still a valid requirement.
- Remove remote access immediately the connection is no longer required or in the event of an IT security breach.
- Have a clear understanding of their responsibilities for security management and administration of remote access.
- Inform the Somerset Partnership Information Management and Technology Team and the Information Security Manager of any IT security breaches/issues.
- Authenticate each remote access user to the system using a strong authentication mechanism as per the Connecting for Health 'Remote Access – Good Practice Guideline' 01/07/2009.
- Ensure the implementation of user profiles and local access controls in accordance with agreed access levels.
- Provide 'out of hours' support for problems related to the access of agreed critical Trust systems.

L2.5 IT Department will:

- Provide remote access solutions using secure virtual private networks (VPN) as defined in the Connecting for Health 'Remote Access – Good Practice Guideline' 01/07/2009.
- Maintain policy and standards on remote access to ensure the identification of risks and the implementation of appropriate controls to reduce those risks.
- Ensure any laptop approved for remote access use has been encrypted.
- Provide incident management and related reporting to the Caldicott and Information Governance Group.
- The IT Department will prepare and configure equipment for remote access, risk assessment, installation or support of equipment at the remote user's location.

L2.6 Trust Board

The Trust Board is ultimately responsible for ensuring that remote access by staff is managed securely.

L3 DEFINITIONS OF TERMS USED

- **ADSL:** Asynchronous Digital Subscriber Line – allows fast data communication over existing phone networks.
- **GPRS:** General Packet Radio Service – always on digital service.
- **GSM:** Global System for Mobile Communications.
- **ISDN:** Integrated Service Digital Network - digital phone network.
- **ISDN Terminal Adapter:** A device to allow connection of a laptop or computer to a network via the ISDN (Digital) telephone system.
- **Kbps:** Kilo bits per second – measurement of data transfer.
- **Mbps:** Megabits per second - measurement of data transfer.
- **Mobile Working:** Using IT equipment to work away from the main site of work but accessing systems on the main site.
- **Modem:** A device to allow the connection of a laptop or computer to a network via the telephone system.
- **Remote Access:** Using IT equipment to work away from the main site of work but accessing systems on the main site.
- **Router:** Device to join two networks together and move data across them.
- **Strong Authentication:** In addition to a user name and password, strong authentication uses a device or text message to generate a code which is accepted by the Remote access system.
- **USB Memory stick:** A very small USB device for transporting files to locations away from Somerset NHS sites. Primarily for the purposes of training or presentation materials, patient information should only be stored on such devices where no other option exists.

L4 PROCESS FOR GAINING REMOTE ACCESS

It should be noted that remote access will only be granted for Trust portable equipment to be connected via the Trust's secure remote access solution.

Personal IT equipment must not be used by staff to gain access to Trust's systems; this is strictly forbidden and could lead to disciplinary action.

Staff requesting use of remote access must ensure that they do the following:

- discuss the need for remote access with their line manager.
- read and understand the Mobile Working Code of Conduct in Addendum (i).
- complete and submit the Remote Access Request Form, found on the Intranet under Forms, IM&T - Intranet.sompar.nhs.uk.
- read and understand Addendum (ii) regarding Risks associated with remote access.

Once the request for remote access has been approved, a copy of the form will be placed on the requester's personal file.

The IT Department will contact the requestor with details of how to connect equipment via the remote access solution.

Addendum (i)

Somerset Partnership NHS Foundation Trust

MOBILE WORKING CODE OF CONDUCT

Remote Access users must NOT:

- Divulge their password or security pin number to anyone.
- Store their password or security pin number on their computing equipment, USB memory stick or in other accessible places.
- Allow others to use their password or PIN.
- Allow unauthorised individuals to use, repair or dismantle NHS computing equipment.
- Allow anyone else to use their computing equipment when logged into the network.
- Log anyone else in using the remote user's user account.
- Install additional software unless directed to by the IT Department, this includes downloading from the Internet.
- Access non-NHS systems, including non-NHS e-mail systems.
- Load or download offensive material.
- Use non-NHS equipment to connect to the NHS network unless specifically approved by the IT Department.
- Change the configuration of equipment or software unless directed by the IT Department.
- Connect to an unapproved non-NHS network with NHS computing equipment.
- Store sensitive information on USB memory sticks. USB memory sticks are for transporting files (training materials or educational course work), not a place to keep things. Especially not sensitive or patient information.
- Place equipment in a location likely to cause loss or damage to the equipment or data eg. damp areas, close to sources of magnetism or heat, insecure areas etc.

Remote Access users must:

Comply with the Trust's IM&T Security Policy. Inform the IT Department immediately of the loss of any NHS computing equipment via the IT Service Desk (**0300 323 0111)** or IT.Services@sompar.nhs.uk

- Ensure any essential data is moved from the mobile device to a network drive when next at their local NHS site.
- Notify the IT Desk if the device's anti-virus software appears out of date.
- Inform the IT Desk immediately if they believe their mobile device has become infected with a virus.
- Use NHS computing equipment for NHS business use only.
- Store equipment in a secure and safe place when not in use.

- Ensure that computer screen or keyboard cannot be overlooked by non-NHS staff when accessing confidentially sensitive systems.
- Protect their password and security pin number.
- Regularly change their passwords on Trust systems, as prompted by the system.
- Comply with all relevant Health and Safety protocols, including the immediate reporting of any hazard.

Addendum (ii)

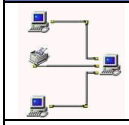
Somerset Partnership NHS Foundation Trust

RISKS

Providing staff with remote access to information systems introduces risks that may have a serious impact for an organisation. Areas of risk involve:

- Loss or corruption of sensitive data;
- Breach of confidentiality;
- Loss or damage to equipment;
- Breach of legislation or non-compliance with regulatory or ethical standards;
- Unavailability of network or resources.

Directory of Risks

Symbol	Business Consequence
	Intruder brings site network services down
	Loss or corruption of sensitive data
	Breach of confidence
	Loss or damage to equipment
	Breach of legal or regulatory or ethical standards

Risk Description	Supporting Information	Consequence
• ***Staff make mistakes through ignorance or negligence***		
Accidental divulgence of information	A malicious third party, who is aware of the relevant User ID etc, may gain access to the network if the remote user unwittingly divulges key information	
Loss of authentication token, or phone used to receive authentication code	A remote user may lose their authentication token, allowing a third party to gain unauthorised access to the network	
Sharing of password with another employee	An unauthorised user may gain access to the network if the remote user shares their password with another employee.	
Use of client computer by family or friends	The remote employee may allow an unauthorised user, either inadvertently or deliberately to use the remote access facilities	
Neglect of important 'housekeeping' activities	Valuable data stored on a client's computer may be lost or corrupted if routine 'housekeeping' activities are not carried out by the remote user.	
Downloading of malicious code from the Internet	Malicious code may be downloaded onto the client computer if the remote user accesses Internet sites	
Introduction of virus from portable media	The remote user may unknowingly introduce a virus onto the client computer if data is loaded from portable media (eg. disk or CD)	

Risk Description	Supporting Information	Consequence
• ***Staff behave in an illegal or offensive manner***		
Unauthorised use of corporate assets	If the remote user makes use of NHS assets for personal purposes, the organisation may be misrepresented.	
Downloading of offensive material from the Internet	If the client PC is used to download offensive material from the Internet, an organisation may be exposed to legal action and its reputation impaired.	
• ***Staff make inappropriate or unauthorised changes to the client computer***		
Loading of unauthorised software	System software may be compromised if the remote user loads unauthorised software onto the client computer	
Unauthorised or inappropriate changes to PC configuration	The computing infrastructure may be unavailable or exposed to the introduction of malicious code if the remote user removes or changes the configuration of software on the client computer	
Unauthorised connection of client computer to a home LAN (Local Area Network), allowing access to other networks	The NHS network may be exposed to unauthorised access or the introduction of malicious code if the remote user connects the client computer to a home LAN which has connections to other networks (eg. Internet)	

Risk Description	Supporting Information	Consequence
• ***The remote location is not physically secure***		
Loss or theft of equipment from remote location	An organisation may be exposed to loss of valuable data or unauthorised access to target information if equipment is lost or stolen from the remote location.	
Damage to equipment in remote location	An organisation may be exposed to loss of valuable data if equipment in the remote location is damaged	
Confidentiality of sensitive data compromised through overlooking	Sensitive data displayed on the screen of a laptop etc may be visible to others.	
• ***Remote location or equipment are not protected adequately***		
Remote location does not meet health and safety requirements	An organisation may face legal action if the remote location does not meet health & safety regulations	
Remote location and equipment are not insured	An organisation may face legal action due to incidents occurring at remote locations, which are not covered by insurance. Eg. An employer's liability insurance may not cover remote locations.	
Restricted use or export of encryption	In some countries a remote user may be exposed to prosecution or confiscation of equipment if encryption is used in the client computer or modem, without appropriate authorisation.	
Data erased by magnetic media	All or some data programs may be erased or corrupted from the hard drive of a laptop if it is placed near a strong electro-magnetic source (eg found on some trains or aeroplanes)	

Risk Description	Supporting Information	Consequence
• ***Client computer is vulnerable to tampering***		
PDA computer lost, stolen or accessor accessed without authorisation	PDA devices are even more susceptible to theft and unauthorised access than conventional laptop computers.	
Discovery of passwords stored on the client computer	Passwords stored on the client computer may be discovered, allowing unauthorised access to sensitive information	
Encryption keys stored on client computer compromised	If encryption keys generated in software on the client computer are compromised, an unauthorised user may gain access to the NHS network	
Removal of client computer hard disk	If the hard disk of the client computer is stolen, sensitive data may be lost	
Removal of client computer back-up battery	An unauthorised user could gain access to the operating system by removing the back-up battery on the motherboard	
Client computer bootable from diskette	An unauthorised user may be able to boot the client computer from a disk and bypass security controls	
• ***Security software is configured poorly***		
Security features of the client computer not configured by default	An unauthorised user may be able to gain access to the client computer if security features are not configured properly	
Inadequate anti-virus protection	Unless anti-virus software is installed, configured correctly and kept up-to-date, the NHS network will potentially be exposed to the introduction of malicious code	

Risk Description	Supporting Information	Consequence
• ***Client connection device is misused or stolen***		
Theft of GPRS mobile phone data (SIM) card	An organisation may be exposed to unauthorised access if an unprotected GPRS mobile phone storing remote access information is stolen. (The SIM card may store telephone numbers and passwords used for remote access)	
• ***Remote staff use communications software in an appropriate manner***		
An unauthorised use of remote control software	An unauthorised user may be able to take control of the network resources with the aid of remote control software (eg. PC Anywhere)	
Unauthorised use of remote network diagnostic tools and protocols	An authorised remote user with privileged access may gain access to restricted parts of the network through the use of remote network diagnostic tools (eg. SNMP)	
• ***Client connection device is not secured***		
Client connection device permanently connected to phone line	An unauthorised user may be able to dial into the client computer if the client connection device (eg. modem) is permanently connected to the phone line.	

APPENDIX M

SAFE HAVEN AND FAX PROCEDURES

1. Introduction

1.1 In order to be able to provide an effective service, the Trust routinely processes personal information. The way in which this personal data is handled needs to be managed in a way that ensures acceptable levels of confidentiality. Such information must be protected so that only authorised staff are able to view or access this information. This is enforced through the Caldicott Principles and the requirements of the Data Protection Act 1998, and set out in the Trust's Confidentiality and Data Protection Policy.

1.2 This Appendix sets out the procedures to follow whilst transferring such data both within the Trust and to external recipients. These procedures also apply whilst receiving information from other trusts or agencies to the Trust to ensure that the data is handled appropriately.

1.3 The transferral of information is known as the Safe Haven procedures and covers the transferal of personal and sensitive data between safe havens.

2. Safe Haven

Definition of a Safe Haven

2.1 A safe haven is a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the Trust to ensure confidential personal information is communicated safely and securely. It is a safeguard for sensitive personal information which enters or leaves the Trust whether this is by fax, post or other means. Any members of staff handling sensitive personal information, whether paper based or electronic, must adhere to the safe haven principles.

Responsibilities

2.2 All staff should be aware of their responsibilities in regards to personal and sensitive information as set out in the Confidentiality and Data Protection Policy and the IM&T Security Policy.

2.3 This covers the handling of confidential and sensitive patient and staff information and applies to all permanent and temporary staff as well as third parties acting on behalf of the Trust.

Purpose of Safe Haven

2.4 The purpose of a safe haven is to ensure that:

- the confidentiality and security of personal information held by the Trust is maintained at an acceptable level. This includes when Trust data is sent to third parties and other partner organisations

- staff are aware that all routine information flows of personal information both internally and externally must be mapped as part of the Trusts ongoing data mapping process by the designated Information Asset Owner. These flows will be risk assessed and reviewed with mitigation being agreed by the Calidcott and Information Governance Group

- all staff and third parties understand their responsibilities in managing patient confidentiality.

Application of Safe Haven Procedures

2.5 Safe haven procedures should be in place in any location where large amounts of personal information is being received held or communicated (e.g. reception areas) especially where the personal information is of a sensitive nature (patient identifiable/ staff information etc).

2.6 There should be at least one area designated as a safe haven at each of the Trust sites where personal information is processed. Where differing teams work then it is expected that within sites further creation of Safe Haven areas may be required or mechanisms are put into place to protect that information so only the relevant team has access to that information in order to meet the Trust's legitimate relationship requirements.

What is a Safe Haven Environment?

2.7 It should be a room that is locked or accessible via a coded key pad known only to authorised staff;

or

the office or workspace should be sited in such a way that only authorised staff can enter that location e.g. it is an area which is <u>not</u> readily accessible to any member of staff who work in the same building or office, or any visitors;

2.8 The room/office should allow for adequate storage for sensitive material, including confidential waste, (whilst waiting for collection) or, where available a Trust approved shredder;

2.9 If sited on the ground floor any windows should have locks on them and windows are not left open when the room is not in use for any period of time;

2.10 The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage;

2.11 Manual paper records containing person-identifiable information should be stored in locked cabinets; or stored in areas where staff only access is possible

3. Use of Fax Machines

General

3.1 Fax machines used for the sending and receiving of sensitive information should be located within the Safe Haven environment.

3.2 Fax machines must only be used to transfer personal information where it is absolutely necessary to do so.

3.3 The fax should always be sent to a safe location where only staff that have a legitimate right to view the information can access it. It is perfectly acceptable to check this requirement is met at the receiving end and is absolutely essential for new flows of information to new fax numbers – even if the third party or organisation is already known.

3.4 Faxes should always be addressed to named recipients.

Sending

3.5 When sending a fax:

- Always check the fax number you are sending to, ensuring that the number is not misdialled and ring the recipient to check that they have received the fax.

- If you are using the number for the first time or only use once, then double-check you know the correct number and double-check you have entered it correctly.

- It is advisable to send a 'test' fax and receive confirmation prior to considering this is a correct number and is especially relevant for the next point (below).

- Where the fax machine has the ability to stores numbers in the memory of the machine then numbers should always be programmed into the machine. However, always check that the number held is correct and current before sending sensitive information.

- You should notify the recipient when you are sending the fax and ask them to acknowledge receipt.

- Remove patient identifiable data from any faxes unless you are faxing to a known safe haven and it is essential to include that information.

3.6 Faxes containing sensitive personal data must not be left lying around for unauthorised staff to see, even within the Safe Haven. This applies both to those sending the information as well as for those receiving it.

3.7 Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier.

3.8 Faxes sent must include a cover sheet, which contains a suitable confidentiality clause – example below:

"*The information contained in this fax is confidential and should not be copied, distributed or disclosed. If this fax has been received in error, please contact the sender and ask the recipient to dispose of this as* ***confidential*** *waste.*"

3.9 It is advisable to check that the recipient does in fact have the ability to properly destroy the information and they know the difference between confidential waste and normal waste. If they are in any doubt ask them to return the information to the Trust either by post or in person (if near a Trust premises).

3.10 If you are in any doubt whatsoever, do not send the fax but make further enquiries. Sending confidential (patient, staff or others) information without such checks can lead to a breach of the Data Protection Act 1998 and either an internal (Trust) investigation or the matter reported to the Department of Health and the information Commissioners Office.

Receiving

3.11 If you are receiving a fax:

- A fax machine used to receive person identifiable or sensitive information must be located in the Safe Haven.

- Faxes should be removed from the machine on receipt. The sender should be contacted to confirm receipt and the fax appropriately dealt with and safely stored.

- If you receive confidential information on your fax machine, it is your responsibility to inform the sender that you have received this information and to deal with this information appropriately.

DOs and DON'Ts of Faxing

DO	DON'T
Telephone the recipient of the fax to let them know that you are about to send a fax containing confidential information. Double-check you have the number correct.	Send faxes to where you know that the information will not be seen for a period of time.
Ask if they will wait by the fax machine whilst you send the document.	Send faxes at times that maybe outside the recipient's hours of work.
Ask for acknowledgement of receipt of fax.	Leave information unattended whilst a fax is being transmitted.
Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential.	Send a fax if you think the number *may be* correct – make sure the number you are sending to is correct.
Check the fax number you have dialled and check again that it is correct before sending.	
Request a report sheet to confirm that the transmission was sent correctly.	
If this fax machine is going to be used regularly, consider storing the number in your fax machine's memory.	