South Central Ambulance Service NHS
NHS Foundation Trust

IM&T POLICIES & PROCEDURES

SECTION 1 – GENERAL CONDITIONS

- **Introduction**
- **Aim**
- **Scope**
- **Statement of Responsibilities**
- **Definitions**
- **Policy Review**
- **Equality Statement**
- **Policy Monitoring**

SECTION 2 – POLICIES

A – Security Access & Control (*was IM&T PP No 5*)
B – eMail Usage (*was IM&T PP No 2*)
C – Internet Usage (*was IM&T PP No 4*)
D – Network Security
E – Anti Virus (*was IM&T PP No 1*)
F – Cyber Security
G – Mobile Device Usage
Z – Incident Reporting (*was IM&T PP No 3*)

APPENDICES
A – Definitions
B – eMail Etiquette = Do's and Don'ts
C – eMail Good Housekeeping
D – eMail Spam and Phishing Hints & Tips
E – eMail Guidelines for Writing
F – eMail Communications with Service Users
G – eMail & Internet Usage – Defamation and Libel
H – Internet Usage – Guidance on Using Social Media
I – Examples of Reportable ICT Incidents
X – ACRONYMS

DOCUMENT HISTORY

Author: **Vince Weldon** – Associate Director of IM&T	**Approval:** IM&T Control Board
This document replaces: IM&TPP No. 1 Anti Virus Ver 003.04 Oct 2013 IM&TPP No 2 eMail Ver 003.05 Dec 2014 IM&TPP No 3 Incident Reporting Ver 003.04 Dec 2013 IM&TPP No 4 Internet Ver 003.04 Dec 2013 IM&TPP No 5 ICT Security Ver 003.04 Dec 2013 IM&TP Control Board Draft Ver 004.01 Nov 2016	**Notification of Policy Release:** Distribution by Communication Managers All Recipients e-mail Staff Notice Boards Intranet Web-site
Equality Impact Assessment:	Stage 1 Equality Impact Assessment – No issues
Date of Issue:	**January 2017**
Next Review:	**January 2020**
Version:	**IM&TP** Version 004.03 Final April 2017

SECTION 1 GENERAL CONDITIONS

INTRODUCTION

This document defines the Information Management and Technology policies for South Central Ambulance Service NHS Foundation Trust (SCAS), The Trust has a requirement to provide and maintain a secure, resilient and adaptable technical information and communication technology infrastructure for the processing of all activities related to its role as a provider of patient care within the NHS. It has a responsibility to ensure the confidentiality, integrity and safety of all patient and corporate records.

This responsibility is defined in the NHS Information Security Policy Guidelines; unless specifically covered by a SCAS IM&T Policy then these guidelines apply.

These policies apply to all functions and information processed by and on behalf of the Trust, the physical and virtual environments in which they operate and the people supporting and using the facilities.

The Trusts intention is to ensure that:

- All staff are aware of their responsibilities in relation to safeguarding the confidentiality, integrity, and availability of data and software within the organisation.
- Best practice concerning the use of software and hardware within the organisation is identified.
- Instructions are provided on best practice to ensure safe and secure access to and use of Trust services

These policies apply to:

- All employees whilst using Trust equipment and accessing the Trusts infrastructure at any location, on any computer or Internet connection.
- Other persons working for the organisation, persons engaged on Trust business or persons using equipment and networks of the organisation.
- Anyone granted access to the network.

ICT facilities are primarily provided to enable staff to perform their duties and to better conduct the business of the Trust. Only ICT equipment which is the property of the Trust and appropriately protected for such use can be connected to the corporate infrastructure.

Every individual defined within the scope of this document is responsible for the implementation of this policy whilst operating any IT equipment to access any of the organisations systems.

Breaches of this policy should be regarded as serious misconduct which could lead to disciplinary action in accordance with the Trusts Disciplinary Policy.

Separate arrangements are provided for staff and visitors to connect non-Trust equipment to Wi-Fi.

In respect of all IM&T Policies and Procedures further advice and guidance can be obtained from the IM&T Department.

1 This Document

Sets out the organisations policies for the protection of its information and communication technology infrastructure, including the confidentiality, integrity and availability of data, the physical and virtual assets that create its infrastructure and the people using these services

It establishes the security and operational responsibilities for the network and associated assets, detailing what personal/private use is permitted using Trust facilities and services.

It provides reference to documentation relevant to these policies

2 Aim

The aim of these policies is to ensure the safe and effective operation of the Trusts information and communications technology (ICT) assets and the information processed. To do this the Trust will:

2.1 ensure availability of equipment and resources
2.2 ensure that end users are authorised and trained to use the facilities provided
2.3 preserve integrity of its equipment and information assets
2.4 provide protection for the network and associated assets from unauthorised or accidental use, modification, access or disclosure to ensure completeness and accuracy of the Trust's assets
2.5 preserve confidentiality
2.6 complement and comply with relevant legislative, statutory and local guidance including but not limited to:

- Data Protection policy
- Confidentiality code of conduct
- Freedom of Information policy
- NHS Information Security and Management guidelines
- Network Security and Access Control policy

3 Scope

These policies apply to all SCAS staff, (including trainees, temporary staff, contractors and consultants provided with authorised access to the Trust's eMail and computer systems) and Non-Executive Directors. It includes any staff not directly employed by the Trust such as community responders or volunteers

These policies apply to all ICT assets in use throughout the organisation for the:

3.1 processing, storage, sharing and transmission of clinical and non-clinical data including images and audio visual recordings
3.2 provision and use of devices, applications, programmes and internet systems for receiving, storing and processing of clinical and non-clinical data, images or audio visual recordings
3.3 printing or scanning of clinical and non-clinical data or images
3.4 provision of hardware and networking facilities for communication, both audio and visual, within and external to the organisation

4 STATEMENT OF RESPONSIBILITIES

4.1 General

ICT facilities have become pervasive across all areas of business life, internal and external to NHS services. ALL staff need to use this service provision in a responsible, effective and lawful manner. All related activity (including internet, eMail, data processing, social media) undertaken on behalf of the Trust remains the responsibility of the Trust. This includes any research or downloading to Trust ICT equipment or e-Mails which an individual may otherwise consider to be personal.

As a publicly funded NHS body the Trust has a responsibility to ensure that the services which it provides are used in a professional and equitable manner for the provision of healthcare. This includes Internet access from the workplace and therefore use of non-work related sites should be restricted during normal working hours, subject to the same managerial controls as any other activity.

Ultimate responsibility rests with the Chief Executive and delegated senior managers of the Trust who are personally accountable for the implementation and compliance of all Trust policies.

4.2 IM&T Department

The IM&T department is responsible for providing and maintaining corporate ICT services and systems and ensuring that: -.

4.2.1 Only authorised users of Trust ICT facilities are provided service provision. A list of all approved ICT users, detailing their service provision and levels of access will be maintained centrally. All authorisation requests must be made by relevant Managers or Directors

4.2.2 Systems are maintained and managed to provide secure and effective access solutions at all times

4.2.3 System access rights are maintained and provided only to duly authorised personnel; this relies specifically on line-managers across the Trust completing the Starters and Leavers protocol.

4.2.4 Automated access controls are in place restricting users to authorised physical and virtual environments. These restrictions will be subject to annual review and approval by the IM&T Control Board. Any amendments to the restrictions requested during the year must be approved by the Associate Director of IM&T or a Head of ICT.

4.2.5 All complaints and breaches of policy concerning the unacceptable use of ICT services on Trust systems are investigated appropriately.

4.2.6 ICT services are used effectively and efficiently through the provision of staff training programmes and the formulation of this policy

4.2.7 These policies are appropriately monitored and implemented across the Trust.

4.3 Trust managers and supervisors

All managers and supervisors have the responsibility to: -

4.3.1 ensure that ICT Access Application Agreements are provided to ICT in respect of all individuals for whom system access is required, this includes timely processing of Starters and Leavers forms for permanent and temporary staff (directly employed and contractors) including any changes required during employment.

4.3.2 implement and monitor the operation of these policies within their functional areas.

4.3.3 ensure that staff follow and adhere to these policies at all times.

4.3.4 ensure that staff are given opportunities for appropriate training and awareness.

4.3.5 sure that all suspected incidents of inappropriate system use are reported and investigated, with corrective action taken as necessary.

4.4 Individual users.

Every user of SCAS ICT services has the responsibility to ensure that they practice appropriate and proper use of the available services, that they understand their responsibilities, and do not bring the Trust into disrepute. All users:

4.4.1 requiring system access accounts or equipment must ensure that managers complete and return appropriate authorisations requests. All agreements must be countersigned by relevant and responsible Managers or Directors.

4.4.2 are responsible in law for any action that they take whilst using SCAS provided equipment and services. This includes being liable for any web-site, forum or chat room use and

misuse, logged under their username and password whether or not this is done during normal working hours.

4.4.3 should understand the appropriate and approved use of internet and eMail services.

4.4.4 must be aware that any data or information that they access or download, and eMail they produce or receive using SCAS equipment and services is not their personal property, but belong to the Trust, and may be subject to public disclosure.

4.4.5 take due care and attention when accessing and inputting information to any system, web-site or forum.

4.4.6 should not distribute or otherwise promulgate non-work related material, especially chain mail, jokes, multi-media presentations, executable files. These should not be downloaded without specific authorisation from the Associate Director of IM&T or a Head of ICT. Please note that this includes ALL music and video downloads, other than for official presentations, and only then where no copyright violation will occur.

4.4.7 should understand their responsibilities under the Freedom of Information Act when using or communicating corporate data and information.

4.4.8 should understand their responsibilities under the Data Protection Act when using or communicating personal data and information.

4.4.9 have a personal common law duty of confidence, and should share information ONLY in accordance with professional standards, local policy and information sharing protocols.

4.4.10 **MUST** understand and comply at all times with related Trust policies including but not limited to those on :

- Data Protection and Confidentiality Policy
- Freedom of Information Policy
- Information Security Policies
- Records Management Policy.
- Discipline and Conduct

Any questions or comments about these Policies must be made in writing to the Associate Director of IM&T or a Head of ICT. If a user does not have any questions the Trust presumes that they understand and are aware of the rules and guidelines and will adhere to them.

The use of Trust ICT facilities by any individual assumes and implies compliance with these policies, without exception. Any misuse of service could result in disciplinary action against individual staff members.

5 Definitions

A full set of definition applicable to the scope of these policies is provided as Annex A

6 Policy Review

These policies will be in place for three years. All breaches of these policies will be reported to the IM&T Control Board, the Information Governance Steering Group, the Trust Executive, the Trust Audit Committee or the Trust Board as applicable. Any changes to legislation, statute or NHS operational guidance which requires a change of policy within the three year period will be considered by the IM&T Control Board.

In the event of significant failure of any policy then that group will approve temporary changes prior to formal review.

7 Equality Statement

The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marital status, disability, race, nationality, gender, religion, sexual orientation, gender reassignment, ethnic or national origin, beliefs, domestic circumstances,

social and employment status, political affiliation or trade union membership, HIV status or any other basis not justified by law or relevant to the requirements of the post.

By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

The Trust will therefore take every possible step to ensure that these procedures are applied fairly to all employees regardless of race, ethnic or national origin, colour or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other relevant factor.

Where there are barriers to understanding e.g. an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resource Department.

8 Policy Monitoring

Use of the corporate ICT infrastructure for business and limited personal use is subject to UK law and the regulations, standards and guidelines issued by the Information Commissioner and Department of Health/National Health Service bodies. Any employee using these facilities illegally or inappropriately could put the Trust in breach of the law, for which the penalties can be severe.

The law requires that monitoring of ICT facility usage complies with the Data Protection Act and the Convention on Human Rights which means that monitoring is kept to a minimum, can be appropriately justified, and that all individuals are aware of this monitoring.

Monitoring will therefore be limited to that necessary to ensure the security of Trust systems and services and to monitor overall usage rather than monitoring of individual accounts and content. Exceptions to this will be in cases where there is a high level of suspicion that the individual(s) is using any system inappropriately. In all cases targeted monitoring may be implemented on receipt of a written request from a relevant Director or Head of Service and following HR advice and policies.

Any monitoring will only be introduced after undertaking an impact assessment and in full compliance of the Information Commissioners Employment Practices Code Part 3 Monitoring at Work 2005. Specifically that authorisation will need to be granted by either the Associate Director of Information Management & Technology, the Director of Finance, Director of HR, a Head of ICT and/or the Caldicott Guardian.

Formal complaints and suspected breaches of these policies will be investigated in accordance with any of the Trusts relevant policies, including but not limited to Disciplinary, Incidents and Near Miss & Risk Management policies. Misuse of the corporate ICT infrastructure provision may, in certain circumstances, be unlawful and could lead to criminal prosecution.

The Trusts IM&T department will be responsible for the monitoring of each policy and it's supporting processes and documentation, reporting regularly to the Trust IM&T Control Board in respect of any incidents and remedial actions taken. Reports on any data breaches will be routinely reported to the Trusts Information Governance Steering Group, and subsequently as appropriate to the Trusts IM&T Control Board, Audit Committee and Executive Group including details of findings and remedial action taken.

9 Date of Next Policy Review: January 2020

SECTION 2 IM&T POLICIES

2A SECURITY ACCESS & CONTROL

1. PURPOSE

Access control is for ensuring that only authorised persons have physical access to hardware and equipment and that their subsequent access to software, systems and information (logical access) is limited and controlled to ensure they are suitably trained and accredited to the level of access provided.

2 PHYSICAL ACCESS CONTROLS

2.1 Physical security protection will be based on defined perimeters and achieved through a series of strategically located barriers throughout the Trust. Critical installations will be protected by, at least, lock and key.

2.2 The requirements and siting of each physical barrier will depend on the value of the assets to be protected, as well as the associated security risks. The security perimeter could define a high security area (such as a sealed off area of the building, a computer room, a locked office) or be based on some other form of physical boundary.

Important or particularly sensitive computer areas must be protected either by manual or electronic locks with codes which can be changed periodically, or by electronic swipe cards where access is restricted on a needs basis. Where key pads are involved codes should only be issued on a need to know basis, with a master code sheet being held securely in the event that emergency access is required.

2.3 Only those staff who have legitimate business and whose jobs require it, should be allowed to enter areas where computer systems are located such as server rooms and data centres. Where an area is designated as a secure area:

- All staff are required to display their SCAS identity card
- Visitors should be supervised, required to wear a visible identification badge, and their date and time of entry and departure recorded in an auditable log.
- Visitors should, if appropriate, be accompanied throughout the visit. Visitors such as contractors, who may be strangers to other staff but need to work unaccompanied, should wear badges and be supervised. Badges should be carefully controlled, including being logged in and out.

2.4 Except in places of public access, staff should be instructed to positively challenge unidentified strangers. Staff should particularly be aware of visitors who are unaccompanied, and not wearing an authorised badge, and should approach them politely to determine their business. As well as protecting against the casual visitor, this will raise staff awareness of the need for security.

The more people who have access to computer installations or to work areas which contain PCs, the more difficult it is to put security measures into effect. Apart from the risk of theft, damage or unauthorised use, data security could be compromised and passwords may become known. When visitors have access to areas where PC's are in use staff are personally responsible for maintaining confidentiality.

2.5 General information on secure areas for the storage and processing of information can be found in the NHS Information Security Guidelines, including the definition and security standards of "Safe Havens".

.

3 LOGICAL ACCESS CONTROL

3.1 Prevention of misuse

Employees of SCAS and any third party users are only permitted access to systems for which they been formally authorised.

The Computer Misuse Act (1990), introduced three criminal offences:

- unauthorised access
- unauthorised access with intent to commit a further serious offence
- unauthorised modification of computer material

Any use of IT facilities for non-business or unauthorised purposes, without the explicit and documented approval of the Associate Director of IM&T or a Head of IT will be regarded as improper use of the facilities and could result in disciplinary action being taken.

All SCAS systems have an identified Senior Responsible Officer/Asset Owner who is responsible for ensuring that logical access controls are in place for each system.

3.2 Third party access

Health organisations are encouraged to share information about patients and, in some cases, to allow access to IT resources by other parts of the NHS and Social Care.

Within SCAS project governance arrangements require approvals to be given for all system developments and procurements. These arrangements ensure that IM&T staff are routinely involved in the decision making process, and actively involved in all projects with an ICT element.

Access to IT facilities or systems by third parties is only permitted where appropriate measures have been implemented and formal information sharing and/or confidentiality agreements have been signed by the third party defining the terms for the connection. SCAS ICT are responsible for undertaking risk assessments on all third party connections to the corporate network, and to recommend counter-measures to mitigate them.

Arrangements for third party access to SCAS computer facilities should be based on a formal contract containing, or referring to, all of the necessary security conditions to ensure that the organisation concerned can satisfy both SCAS and NHS security requirements.

3.3 Protection of data

3.3.1 Access to operational application systems is limited to authorised users and all systems containing personally identifiable or business/commercially confidential or sensitive data must be subject to access controls – as a minimum individually named users will have unique sign-on passwords, while access to test programs is limited to identified development staff.

3.3.2 Maintenance and ICT support staff do not have routine access to live files, even for copying purposes, unless otherwise unavoidable.

3.3.3 The access control procedures which apply to operational application systems also apply to test application programs

3.3.4 There must be a separation of duties for “live” records between end user staff and those with maintenance responsibility to ensure that data is processed safely. When data is required by programmers or developers then copies should be taken and provided. Failure to separate responsibilities in this way increases the risk of procedures being evaded for expediency, with subsequent loss of confidentiality.

3.3.5 The copying, archiving or dumping and deletion of any data should be authorised by the data owner and copies should be treated as having the same level of security and access restrictions as the originals.

3.3.6 Live sensitive data should not be used for testing, training or demonstration purposes unless it is transformed such that identification of any individual is not possible. (NHS Information Governance Standards in respect of Pseudonymisation of Data will be followed at all times)

3.3.7 This applies in particular to all personal data as defined by the Data Protection Act 1998 (DPA). If live personal information is being "transformed" to use for test purposes, simply changing a name is not sufficient protection. If a person could be identified by anyone, from the rest of the data (for example, medical history, address or other personal details) then all the data must be transformed. Live and test data files should always be logically separated.

3.3.8 Live and test data should, where possible, be physically separated. Where this is not possible, then the data should be logically separated by being placed in separate partitions or directories or the equivalent. If data is to be moved between live and test environments then the migration should be strictly controlled. An automatic log should be produced and audit trails maintained.

3.3.9 For all systems a record of access rights, identified system managers, test and live environment arrangements and exceptions to this policy must be maintained. This is a responsibility of the acknowledged systems asset owner which is overseen by IM&T who will maintain a central record of ALL systems which is reviewed annually by the IM&T Control Board.

3.4 Data classification

The Senior Responsible Officer/Asset Owner for each system is responsible for:

- identifying all the data within the area of responsibility
- specifying how the data can be used
- agreeing who can access the data, and what type of access each user is allowed
- determining the classification or sensitivity level(s) of the data
- periodically reviewing that classification
- approving appropriate security protection for the data
- ensuring compliance with security controls
- ensuring compliance, where necessary, with the Data Protection Act 1998, and any other relevant legislation covering personal or medical data

Data which contains personal information in respect of patients or staff members which is not otherwise freely available in the public domain should always be treated as confidential. Where the information relates to a medical diagnosis or private matter then it should also be treated as sensitive.

Data classed as sensitive or confidential within one system should maintain at least the same sensitivity level across all systems.

Access rights given to users should be consistent across all areas. Particular attention should be paid to data being downloaded to a PC or laptop – permanent storage of data on such devices is not encouraged as only data that is held in network storage areas is routinely and regularly backed up.

Classified information should be labelled appropriately and output from systems handling any classified data should carry an appropriate classification label (in the output).

The marking should reflect the classification of the most sensitive data in the output. Output includes printed reports, digital media, electronic messages and file transfers.

Information often ceases to be sensitive after a period of time, for example, when the information has been made public. This should be taken into account, as over-classification can lead to unnecessary expense.

3.5 User registration

All SCAS information systems are subject to formal, documented user registration and de-registration procedures governing end user access. These procedures should:

- check that each user has authorisation from the system owner to use the service
- check that the level of access is appropriate for the business purpose and is consistent with the organisational security policy
- ensure that service providers do not provide access until the authorisation process has been completed
- maintain a formal record of all persons registered to use the service
- immediately change or remove the access rights of users who have changed jobs or left the organisation
- periodically check for, and remove, redundant user-id's and accounts that are no longer required
- ensure that redundant user-id's are not re-issued to another person

System owners are responsible for undertaking a formal annual review of users' access rights which will be subject to audit and subsequent reporting to the Trust Audit Committee through the IG Steering Group Annual Report. The process should ensure that access rights are reviewed regularly and that authorisation for special privileged access rights are reviewed more frequently.

Each user should have a unique identifier (user-id) for their personal and sole use. A unique user-id ensures that all activities on the system can be traced to the individual responsible. The user-id should not indicate whether a user is a manager, supervisor or has special privileges.

3.6 Privileged access

The use of special privileges must be restricted and controlled. "Special privileges" are those such as are allowed to the system manager or systems programmers, allowing access to sensitive areas (for example, passwords). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached.

For multi-user systems, the allocation of special privileges will be controlled through a formal authorisation process, which will:

- identify the special privileges associated with each system product (for example, operating system, database management system) and the categories of staff to which they need to be allocated
- allocate special privileges to individuals on a "need to use" basis and on an "event by event" basis - i.e., the minimum requirement for their functional role and only when needed
- maintain a record of all special privileges granted. Privileges should not be granted until the authorisation procedure is complete
- ensure that any user assigned special privileges for a particular purpose uses a different user identity from that used for normal business purposes and is allocated a "one-off" password, which is deleted after use

3.7 Password control

All systems containing personally identifiable data or sensitive business information must be subject to end user password access controls. All new users must be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected.

3.8 Password application

Each member of staff will be provided with a unique network identity and password and be informed that they are *personally* responsible for all activity within their own logon account.

For the most effective security, staff should have self-selected, individual passwords within defined parameters.

Passwords must be changed regularly. This should be at least every **sixty** days or as specified in the secure operating procedures for the system. Where possible, this change should be enforced by the system. Each time a password change is made a new and unique password should be used. Passwords should always be changed immediately on suspicion of any compromise.

The longer a password remains unchanged, the more opportunity a potential intruder will have to discover it. Once compromised a password will continue to allow access until it is changed.

3.9 Automated password management

Where possible, an effective, automated password system to authenticate users will be implemented. To ensure better security a good password system should:

- enforce the use of individual passwords to maintain accountability
- allow users to select and change their own passwords and include a confirmation procedure to allow for typing errors
- enforce a minimum length for passwords (at least six (6) alpha numeric characters are recommended)
- where users maintain their own passwords, enforce a password change at regular intervals. A maximum of sixty days is recommended, with users being prompted to change their passwords during the seven days prior to the expiry date
- where necessary, enforce a more frequent password change for privileged accounts, for example, those with access to system utilities
- where passwords are selected by the user, force them to change temporary passwords at the first log-on
- maintain a record of previously used passwords, for the past twelve months, and prevent users from re-using them
- not display passwords on the screen when being entered
- store password files separately from the main application system data
- store passwords in encrypted form, using a one-way encryption algorithm
- alter vendor default passwords immediately after installation
- check that the user has selected a quality password, by checking, for example, that the password does not include any of the following:
  - months, days, or any other date aspect
  - company name
  - user-id, user name, group-id or other system identifier
  - two or more consecutive identical characters
  - all numeric or all alphabetic groups

4 Log-on procedures

Access to IT services should be via a secure log-on process, designed to minimise the opportunity for unauthorised access. The log-on process should:

- not display system or application identifiers until log-on has been successfully completed
- display a general notice warning that the computer should only be accessed by authorised users and that access by unauthorised users may constitute an offence under the Computer Misuse Act (1990), for which they may be prosecuted
- not provide, during log-on, help messages that would aid an unauthorised user
- validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect

- limit the number of unsuccessful log-on attempts allowed to three (3), after which the following actions should take place:
  - the unsuccessful attempt is recorded
  - a time delay is forced before further log-on attempts are allowed
  - data link connections are disconnected
- limit the maximum time allowed for the log-on process. If exceeded the system should terminate the log-on
- display the following information on completion of a successful log-on:
  - date and time of the last successful log-on
  - details of any unsuccessful attempts since the last successful log-on

Where it is important that a session should be initiated only from specific locations automatic terminal identification should be implemented.

An identifier in a terminal can be used to indicate whether a particular terminal is permitted to initiate or receive certain transactions.

5 Time-out procedures

Inactive devices should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions. Use of a Windows™ Screen Saver to time-out a PC-based application should always be set up to require the input of the user's password to reactivate the screen.

A high risk area might be a public or external area outside the control of SCAS security management. The time-out delay should reflect the security risks of the area. In such areas, a maximum time-out period of 5 minutes should be set.

Users should log off terminals or PCs when leaving them unattended. PCs or terminals should be secured by a key lock or equivalent control (for example, password access control) when not in use.

For high risk applications, connection times should be restricted. Limiting the period during which terminal connection to IT services are allowed reduces the window of opportunity for unauthorised access. This should be considered for sensitive systems.

A restriction could be:

- using predetermined time slots
- restricting connection times to normal office hours if there is no requirement for overtime or extended hours operation
- limiting the elapsed time for any connection

6 Data and information access

Access to data and information should be granted only to staff who need to use it to perform their job function. This applies particularly to security data which should be accessed only by security staff. Security data includes password files, encryption and authentication algorithms and user profiles.

If data access rights are changed or by-passed a report should be produced showing:

- the identity of the person making the change
- the reason for the change
- what is being changed
- who would or could be affected by the change

- the date and time of the change

If the mechanisms have been bypassed by an unknown intruder then the incident should be treated as a breach of security and fully investigated.

Except in emergencies, staff should not be granted access to live data over and above that originally assigned by the data owner. Where emergency access rights are granted (for example, to technical support staff or engineers) they should always be granted under a specially allocated user-id and be password controlled. The password should be changed on completion of the emergency activity. All activity during the emergency should be automatically monitored and covered by logs and audit trails.

All detected unauthorised attempts to access systems or data should be reported to the Associate Director of IM&T or a Head of IT as a security incident.

Access restrictions should also take into account the classification of the data stored on or processed by a particular application and apply appropriate control procedures.

7 System utilities restriction

The use of system utilities (tools which can be used to change settings within computers) should be restricted and controlled. System utilities can be capable of over-riding system and application controls. Therefore the use of those utilities should be restricted to those who **need** to use them and their use controlled by the following:

- password protection for system utilities
- segregation of system utilities from applications software
- limitation of the use of system utilities to the minimum number of SCAS, authorised users
- limitation of the availability of system utilities, for example, for the duration of an authorised change
- logging of all use of system utilities
- defining and documenting authorisation levels for system utilities
- removal of all unnecessary utility and system software

In order to minimise the possibility of corruption of computer programs, strict control should be maintained over access to program source libraries (the place where original operation programme code is secured) as follows:

- where possible, program source libraries should not be held in operational systems
- a program librarian should be nominated for each application
- IT support staff should not have unrestricted access to program source libraries
- programs under development or maintenance should not be held in operational program source libraries
- the updating of program source libraries and the issuing of program sources to programmers should only be done by the nominated librarian upon authorisation from the system manager. If emergency re-compilations need to be done without prior SCAS, a record of all the circumstances should be kept for subsequent investigation
- program libraries should be held in a secure environment
- an audit log should be maintained of all accesses to program source libraries
- old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures

- maintenance and copying of program source libraries should be subject to strict change control procedures

Vendor supplied software packages should be used without modification. If any changes are necessary, these should be obtained from the vendor and subjected to controlled implementation involving appropriately qualified SCAS employees.

8 Remote access/access from non-NHS networks

Remote access over PSTN (Public Switched Telephone Network) and ISDN (Integrated Services Digital Network), and access from non-NHS networks to the SCAS network is not allowed as a matter of practice: where it is provided it must be subject to strong authentication procedures, and only undertaken with the explicit and documented authorisation of the Associate Director of IM&T or a Head of IT

8.1 Remote/external access by SCAS employees

Where a SCAS employee is working on SCAS or client data away from SCAS premises, with the appropriate authorisation, they may need to link to SCAS applications in order to process, upload or download data. Such access should be:

- Specifically authorised by the employees Head of Service or Director.
- Strictly controlled to authenticate the identity of the user through the use of a VPN solution (Virtual Private Network) which has been approved by the Associate Director of IM&T or the Head of IT and endorsed by the IM&T Control Board. The VPN solution will require authorized users to utilize a unique user password, relevant token or software authentication. No individual will be provided with VPN access if they are not in possession of an up to date NHS Information Governance certificate

8.2 External access by Software suppliers

Suppliers of software applications frequently require remote access in order to perform software updates, e.g. to repair known problems (bugs). No such access will be allowed without notification to the ICT team seeking authorisation, defining the activity to take place and the time and duration anticipated for the connection.

Contracts with software suppliers or managed and outsourced facilities organisations should include the requirement that no direct remote access to SCAS applications is permitted without such authorisation.

8.3 Access by other NHS organisations & networks

The rules governing access by other NHS organisations, such as information required for statistical collection, medical research projects etc., are compliant with the requirements of the Health Service Guidelines relating to the Protection and Use of Patient Information and access must be authorised by the Associate Director of IM&T or a Head of ICT.

Access controls must be applied as described above.

SECTION 2 IM&T POLICIES

2B eMail POLICY

1 PURPOSE

SCAS eMail is primarily provided to enable the sharing and exchange of work related material. eMail has become the main written business tool for both internal and external communications and as a result should be treated with the same level of attention given to drafting and managing formal letters and correspondence.

As well as taking care over how eMail messages are written it is necessary to manage eMail messages appropriately after they have been sent or received.

Whilst it is acknowledged that some personal use of the eMail system is inevitable staff must not abuse that facility. All eMail generated from within the SCAS service carries information which clearly identifies the organisation as being a point of origin.

Misconceptions about how eMail messages can be used could result in legal action being taken against the Trust or individuals. All eMail messages are subject to Data Protection and Freedom of Information legislation and can form part of the "corporate record" of the Trust. As such they can be disclosed and used as evidence in legal proceedings.

This eMail policy sets out the obligations that all members of staff have when dealing with eMail. It covers the sending, receiving, forwarding and storing of all eMail messages, whether internal or external.

2. LEGAL FRAMEWORK

2.1. General

Although eMails seem to be less formal than other written communication, their legal status is the same. Users must be mindful of these at all times, especially when communicating in respect of agreements, contract terms and variations.

As part of the written corporate record of the Trust they are subject to legislation such as the Data Protection Act (1998), the Freedom of Information Act (2000) and the European Convention on Human Rights 1988. As such eMails may be released in part or whole to a wider audience or used as evidence in legal proceedings.

This means that care should be taken with regards to ensuring that users do not:

- Send or forward messages or attachments that contain remarks or depictions that could be deemed libellous, defamatory, offensive, harassing, racist, obscene or pornographic
- Breach the Data Protection Act 1998
- Send or forward information in breach of Copyright legislation

2.2. Formation of Contracts

As indicated in 2.1 above eMail correspondence can be used in the forming of contracts and legally binding agreements. Users must be mindful of this at all times.

The Trust will be held liable for any representations made or contractual arrangements entered into by its employees if it is reasonable to assume that such employees were acting with the employer's authority.

The following Acts of Parliament are particularly relevant to this policy.

Data Protection Act 1998

The Data Protection Act 1998 protects personal data, which includes information about staff, patients and carers. The Trust relies on maintaining the confidentiality and integrity of its data to maintain the trust of the community. Unlawful or unfair processing of personal data may result in the Trust being in breach of its Data Protection obligations. This includes personal data within eMails.

Human Rights Act 1998

Article 8 of the European Convention on Human Rights creates a right to respect for private and family life and for correspondence. This needs to be considered in line with any eMail monitoring arrangements that the Trust wishes to put in place.

Freedom of Information Act 2000

Any information that is held by the Trust may be subject to disclosure under the Freedom of Information Act 2000. There are some limited exemptions in place, but there is a chance that eMails sent and received by Trust staff may be seen by those for whom it was not originally intended.

Copyright Act 1988

Under the Copyright, Designs and Patents Act 1988 copyright law can be infringed by making an electronic copy or making a "transient" copy (which occurs when sending or forwarding an eMail). Copyright infringement is becoming more commonplace as more and more people forward text, graphics, audio and video clips by eMail. Employees must not therefore copy, forward, or otherwise disseminate third-party work without appropriate consent.

3 IT FRAMEWORK AND CONTROLS

3.1 Core Principles

3.1.1 All Trust staff will have access to scas.nhs.uk eMail facilities.

3.1.2 All staff will have the ability to request an nhs.net eMail, which is a pre-requisite for the sharing of clinical information with other NHS organisation s

3.1.3 Limited personal use will be allowed within the confines of this policy framework.

3.1.4 Safeguards will be established to protect the security, integrity and availability of the Trust's systems.

3.1.5 The requirements of the relevant Acts of Parliament and mandatory national policies will be observed at all times.

3.1.6 Staff awareness of copyright and contractual issues will be raised.

3.1.7 Guidance on eMail etiquette's will be provided (Appendix B)

3.1.8 Guidance on housekeeping to ensure efficiency in the operation of the network and personal folders is provided in this policy.

3.2 Risks associated with the use of eMail

The very nature of eMail systems set against the legal framework at Section 2 means that there are a number of potential risks to the individual and the Trust associated with the use of eMail.

For example

- eMail messages can easily go to persons other than the intended recipient, and if confidential or sensitive could be damaging to the Trust.

- eMail messages can contain computer viruses, which are particularly damaging to the Trust's computer systems.
- letters, files and other documents attached to eMails may belong to others and there may be copyright implications in sending, forwarding or receiving them without permission.
- eMail is fast and as such messages written in haste or written carelessly may be sent without the opportunity to check or rephrase. This could give rise to legal liability.
- an eMail message may legally bind the Trust contractually in certain circumstances without proper authority being obtained internally.
- eMails should be regarded as potentially public information, which may carry a heightened risk of legal liability for the sender, the recipient and the Trust.

3.3 IT Controls

There are a number of safeguards and controls built into the eMail system to protect it from overload, keep data storage to acceptable levels for disaster recovery and ensure fair, appropriate and consistent use by all staff across SCAS.

These safeguards and controls are also dependent on good user practices and housekeeping measures. eMail systems are communication tools and not central filing systems. Individual eMails should always be considered as transient, used only for carrying information in the short term. It is the users' responsibility to ensure that the eMail system is not used to store non-work related material and that work related eMails are actioned, deleted or transferred into a more appropriate filing location.

More guidance on effective eMail housekeeping is given in Appendix C.

To prevent loss of information eMail messages must be acted upon and moved to a more appropriate location as quickly as possible.

3.3.1 **Message Limits**

Incoming and Outgoing message size is generally limited to files of 10MB. If you have an eMail that exceeds this limit, consider breaking it down into smaller eMails or removing unnecessary items such as graphics/pictures.

In special circumstances this restriction can be lifted, temporarily, by seeking permission from the Associate Director of IM&T or a Head of IT. Where the distribution of such a document is internal then it would be advisable to utilise the Intranet or shared network storage space to avoid unnecessary duplication within the eMail system

3.3.2 **Mail Box Limits**

As a standard each user is provided a mailbox size of 250MB.

When this limit is reached, the user will receive a warning message of such and will be unable to **send** or forward any eMail until they have brought their mailbox below this limit. The user is able to receive inbound eMails until their mailbox reaches 500mb and then they will not be able to receive or send any further eMails. ICT staff will routinely review mail box usage and report to relevant managers any instances where mail is not being managed appropriately.

Exceptions to this limit, to a maximum of 1GB, can be provided on the authorisation of the relevant Director or Head of Service who identifies an operational need to do so.

3.3.3 **Distribution List Limits**

Standard distribution lists for the circulation of work related material will have an attachment size limit of 8mb to prevent unnecessary duplication within the system. Alternative methods should be

considered such as publishing such documents on the Trust Intranet or Staff Notice Boards. Files containing graphics and pictures can be unusually large. These should be removed if unnecessary.

The use of "ALL" distribution is limited to the Chief Executive and key HR and Communication post holders. Any exceptions to this can only be authorised by the Chief Executive, the SIRO (Senior Information Risk Owner) or the Associate Director of IM&T. All exceptions will be periodically reviewed.

It is anticipated that local distribution lists for divisions, work groups, professional groups etc. will be managed by appropriately trained and authorised individuals, who will be responsible for maintaining the accuracy of such groups. IM&T resources will regularly review the use and management of such groups and take all and necessary appropriate action in the event that the facility is abused. This can include removal of local rights and/or disciplinary action where the misuse can be demonstrated to have been vexatious or deliberate.

Inappropriate use of eMail distribution lists waste both network resources and staff time, for this reason they are to be used solely for distributing work related information which is relevant to everyone on the list and cannot be communicated effectively by any other method. Any abuse of this facility will be reviewed and offending individuals instructed to recall their message. Their action will be reported to their line managers and where applicable additional measures will be requested.

3.3.4 Security Controls – Virus and Hoax Notifications

Although the Trust scans all inbound and outgoing messages for suspect viruses the possibility remains that infected messages can go undetected, therefore:

- In the event that a user suspects a virus is attached to a received eMail they must stop using their machine and contact the ICT Help Desk immediately logging the call as urgent.
- Users should not open eMail messages or attachments from sources that they do not recognise or that they are not expecting
- Users should not open attachments, web links or executables from sources they are unsure of. If in doubt, contact the ICT Help Desk or delete the message without reading and empty from your recycle bin.
- ICT will review any potentially infected eMail and either quarantine the device or cleanse it. No device should be used until all suspicion has been erased.
- To minimise the threat of potential virus attack the Trust will routinely set its filtering system to block eMails which contain attachments with non-standard file extensions and encrypted zip attachments as these can be used to distribute unsafe file types.
- Files that execute a set of instructions to install or delete files etc. (including executables, visual basic scripts and batch files) will normally be removed from eMail messages and replaced with messages indicating that potentially unsafe attachments have been removed (*some exceptions will be included within standard operating routines – for instance the sharing of media files within the Communications team however should these exceptions be abused then individuals will find themselves subject to Trust disciplinary procedures*) These conditions can also be applied to audio, video and photo files.
- Because security risks can change rapidly these restrictions can and will be modified without notice, but all changes will be routinely reported to the IM&T Control Board
- Users should ensure that the latest anti-virus software is available to them. It is a disciplinary offence to ignore requests to accept an anti-virus update

There is no routine scanning of eMail exchanged within the SCAS network, it is imperative that all staff remain vigilant accordingly. It is a disciplinary offence to knowingly breach SCAS protocols and introduce any computer virus into the Trust infrastructure.

It is also not advised for anyone other than IM&T to issue or forward any "virus warnings" internally or to external contacts. It is extremely unlikely that users will be aware of genuine threats before ICT or the Trust's anti-Virus providers. IM&T Staff will always check the validity of received warnings before releasing them publicly.

Any exceptions to these controls MUST be approved by the SIRO, the Associate Director of IM&T or a Head of ICT. Exceptions will be reviewed by the Trust IM&T Control Board and as appropriate included within standard operating routines or removed.

3.3.5 Back-ups

The IM&T division seek to back up the eMail servers regularly for the purposes of business continuity and as part of their disaster recovery assurance programme.

This does not mean IM&T will recover accidental deletion of eMail related items due to the time and processes involved. Users should not be offended if a request is denied.

Personal folders can be used to store eMail related items. Staff working from a single base, or mobile staff using laptops, can make temporary use of their PC/laptop storage facilities, but should store all required data permanently in their network file area. IM&T cannot guarantee recovery of such items in the event of equipment failure – individuals are responsible for their own back ups of locally held material. Staff working on shared data are required to use network storage space, which like the eMail servers, is routinely backed up.

The eMail system is for communication, not for storage. Please use other methods for storing eMails.

4. Unsolicited eMails / Spam / Phishing

IM&T deploy various Anti-Spam software tools to block "junk mail" sent by suppliers or other bodies which may contain emerging threats and offensive content within the eMail body or attachments. Messages can be deleted or quarantined for approval. A series of tips for users to consider are attached as Appendix D.

5. Disclaimer

All eMail messages sent externally must contain the following disclaimer (which will be automatically added to the bottom of every outgoing eMail – staff should therefore NOT use their own versions of disclaimer notices): -

Disclaimer: The information contained in this message, or any of its attachments, is privileged and confidential, and is intended exclusively for the addressee. The views expressed may not be official policy of the South Central Ambulance Service NHS Foundation Trust, but the personal views of the originator. If you are not the addressee, any use of this communication is not authorised. If you have received this message in error, please advise the sender immediately and delete.

All eMails received and sent by this trust are subject to the Freedom of Information Act 2000 and therefore may be disclosed.

Additional information can be added for particular marketing or advertising purposes but only with the approval of the Communications department to ensure corporate standards are maintained.

6 Personal Use

Limited personal use of corporate eMail facilities is currently permitted provided that full compliance with this policy is maintained. Employees should regard this facility as a privilege that should normally be exercised in their own time without detriment to their working performance.

The Corporate eMail system is NOT to be used for personal gain, group mailing of non-work related material or the promulgation of non-work related material

Inappropriate or excessive use **WILL** result in disciplinary action and/or removal of facilities.

Staff should be aware that use of eMail might be subject to monitoring, and disclosure to others. In order to respect and protect the privacy of individuals in compliance with the European Convention on Human Rights it is strongly advised that all personal/private eMails: -

a) are not stored in Mailboxes or Personal Folders but are actioned and deleted immediately from all mailboxes
b) should be clearly marked as "Personal" in the subject heading/title of the eMail. In addition, as much as is practically possible, incoming eMails should also be marked in the same way.
c) set the Sensitivity flag to 'Personal' in the Options tab within the eMail.

Remember that the mail system is a working business communications tool – not a home personal provision. eMail marked as Personal will NOT be exempt from monitoring or reporting procedures.

7 Access to Individual Mailboxes

There are occasions when it is necessary to access eMail messages from an individual's mailbox and when eMail messages sent or received may be seen by others e.g. when a person is away from the office for an extended unplanned period, has left the organisation or simply in the interests of business continuity.

The reasons for accessing an individual's mailbox can be to action the following:

1. Line of business and business continuity issues
2. Subject access requests under the Data Protection Act
3. Information requests under the Freedom of Information Act
4. Evidence in legal proceedings
5. Evidence in criminal investigations
6. Evidence to support disciplinary action

The more formal investigations and breaches of security/inappropriate use of systems (Nos 4-6) will be handled in accordance with NHS Information and Security Management guidelines.

The procedure to be followed to ensure business continuity and compliance with Information Access Regimes (Nos 1-3, 6) is as follows.

1. Gain written authorisation from a relevant Director or Associate Director/ or delegated Head of Department (not simply line manager as it is likely that the Line Manager will be the source of the request). The need for access must be justified and in keeping with the Data Protection Act, the Convention on Human Rights and the Information Commissioners Office: Employment Practices Code Part 3 Monitoring at Work 2005. If in any doubt contact the Information Governance Manager for clarification.
2. The authorised officer must submit a written request (including eMail from the officers' personal account) to the SIRO, Associate Director of IM&T or a Head of IT, and other than for discrete

investigations for disciplinary investigations, to the ICT service desk outlining the reasons for the access request. The ICT Service Desk will nominate a named technician to respond

3. Other than in cases where discrete action is required for disciplinary investigations the Line Manager shall write to the individual to advise that their account has been accessed, providing an explanation why and advising on actions to be taken on the individuals return to work.
4. On accessing the mailbox any investigating or delegated staff should:
   - Ensure that the eMail monitoring is confined to address/heading unless it is essential for a valid and defined reason to examine content
   - Wherever possible avoid opening the content of any eMails, especially ones that clearly show they are personal or private. Only in exceptional circumstances should eMails that are clearly marked personal be opened, for example if the worker is suspected of using the eMail system to engage in criminal or inappropriate activity.

The ICT Service Desk will handle all forms and processes in relation to these access arrangements.

NB. This procedure should not be seen as the "norm" as issues of confidentiality and privacy need to be understood and followed.

The recommended most effective way to ensure business continuity and access to appropriate information when required is for individuals to use the Permissions Tools within Outlook to grant mailbox access to work colleagues, personal assistants, and/or other members of their team etc. so that someone can monitor and respond to eMail messages during periods of absence, ensuring that is it "business as usual" at all times.

All instances of Authorised Access (other than for those staff who have left the organisation) will be reported through the Information Governance Steering Group.

8 USE OF EMAIL FACILITIES

The Trust encourages and supports the use of eMail as an appropriate business tool for internal and external communications. It is vital that eMail is used effectively and appropriately at all times by all staff.

8.1 When eMail is prohibited.

Whilst there are times when the use of eMail is not the best option for communications or information sharing there are other types of eMail use that are **expressly prohibited.**

This includes any behaviour or comments that are not acceptable in the spoken or paper environment as these are also not acceptable within the eMail environment; this includes the transmission (i.e. sending, receiving or forwarding) of any material that: -

1. Brings the NHS or Trust into disrepute.
2. Is abusive, threatening or serves to harass or bully others.
3. Discriminates or encourages discrimination in any way including grounds of ethnicity, racism, gender, sexual orientation, marital status, disability, political or religious beliefs.
4. Contains offensive, obscene or indecent images, data or other material.
5. Contains unsolicited commercial or advertising materials, chain letters, jokes or junk mail of any kind.
6. Contains software files that execute a set of instructions e.g. executables, batch files or visual basic files
7. Infringes copyright of another person including intellectual property rights.
8. Wastes staff effort or networked resources.
9. Corrupts or destroys other users' data or disrupts the work of other users.
10. Violates the privacy of others.

11. Attempts to disguise the identity of the sender, is anonymous or is deliberately forged.
12. Distribution of non-work related eMail, internally and/or externally, including “For Sale” or “wanted” items and sponsorship appeals

In addition it is important to understand that eMail messages containing inaccurate information about an individual or organisation may result in legal action being taken against the person sending the eMail message and anyone forwarding the eMail message on to others.

The transmission of eMails that include any of the above could result in formal disciplinary proceedings being taken against the person sending the message and anyone forwarding the eMail message to others.

8.2 When should eMail not be used?

There are other circumstances when eMail is not always the best way to communicate information as eMail messages can often be misunderstood by the receiver and the volume of eMail messages people receive can be counter-productive and result in work overload. This may mean that a meaningful and productive response is not always possible.

The decision to send or forward eMail or use other communication methods rests with the individual but consideration should always be given to the **appropriate communication method to be used.**

For example: -

- eMail messages should never be regarded as totally secure. Guidance on using eMail for confidential/sensitive or personal data is covered in Appendices B-G inclusive

- eMails should be kept as short as possible. This is particularly important when sending or forwarding messages to large mail groups.

- Send or forward eMails only to those people that need to see them, as sending eMails to all in your address book, or replies to everyone who received a replicated original is both time wasting for inappropriate recipients and can unnecessarily block the system.

- Files such as word documents and spreadsheets are generally quite large so attaching files to messages should be minimized as far as possible.

- Understand the eMail implications whilst at home:
  - Access to the corporate eMail infrastructure via secure external links, utilising domestic and commercial broadband services is available to staff where the need can be justified, and a formal written request is received from the relevant head of service, assistant Director or Director.
  - The transfer of documents or information from SCAS services to domestic or personal eMail accounts is not condoned.
  - Only documents and information that relate to work undertaken on behalf of the Trust may be exchanged between work accounts. No personal files or personal eMails should be sent to home accounts.
  - Remember that these documents are the property of the Trust and master documents/unique copies/records should remain within the Trust’s main filing structures and networks, and not on home computers or laptops.
  - It is strictly forbidden to send or forward any files that contain **person** identifiable information i.e. health care records or confidential patient level information to non-NHSnet or similarly secured accounts. Any breaches of this will be the subject of disciplinary action.

- Do not send or forward eMail using another person’s eMail account unless you have permission and formally authorised access to their account.

- Sending or forwarding eMail messages that contain adverts, congratulations, Christmas cards and greetings etc. to multiple eMail addresses must be avoided.

- Sending generalist eMail messages to large Trust-wide groups should be avoided where possible especially if the messages contain attachments. Remember that one person's piece of important information is another's junk eMail.

- If you have information or documents that you want to send to a wide audience put the information and documents on the intranet and then simply send an eMail containing the link to that updated information.

- This is particularly pertinent for those regular publications such as newsletters, updates, minutes, policies, prospectus's etc.

8.3 eMail etiquette - creating effective and appropriate eMails.

When writing business eMail messages it is important that consideration is given to the way in which the message is being conveyed. The same conventions used in traditional written methods of communication also apply to eMail.

e.g... Dear Dr J Smith etc.

Appendix E presents Guidelines for Writing Effective and Appropriate eMail Messages

9 SECURITY AND CONFIDENTIALITY

9.1 Confidentiality

Confidentiality can be compromised especially when using external Internet-based eMail systems and the privacy and confidentiality of messages sent via eMail cannot be guaranteed. It is the responsibility of all members of staff to exercise their judgement about the appropriateness of using eMail when dealing with sensitive or confidential subjects.

NB. - Home working/working whilst at home

Confidential and/or sensitive information or data must not be copied or removed from the workplace unless specific authorisation has been given. Any confidential and/or sensitive information that is copied or removed from the workplace should be subject to approved procedures designated to minimise the risk of loss or disclosure.

9.2 Sensitive Information

Staff must ensure that all information of a sensitive nature that is sent via eMail is treated with care in terms of drafting and addressing. Sensitive information sent via eMail that is incorrect might provide a case for initiating legal proceedings against the person sending the information and/or the Trust. Sensitive information can include commercial information, information about specific individuals or groups and patient information

When sending or forwarding eMail messages that contain sensitive information the following aspects MUST be considered:

- eMail messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message, for example an eMail message containing comments about the performance of a specific staff member or a group

of staff. This should decrease the likelihood of the message being forwarded to unintended recipients.
- eMail messages that contain information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.

9.3 Personal data

When sending eMail messages containing **personal data** the following aspects MUST be considered

- EMail messages containing personal information are covered by the Data Protection Act and must be treated in line with the principles outlined in the Act.
- Under the Data Protection Act personal information includes opinions about an individual or the personal opinions of an individual. EMail messages containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, and must not be disclosed to third parties without the express permission of the individual concerned.

9.4 Communications with Service Users: Ensuring Compliance with the Data Protection Act 1998.

EMail outside the NHS net is an insecure method of communicating, and confidentiality cannot be guaranteed, however service users are increasingly requesting eMail correspondence for a variety of different reasons.

a) They simply prefer eMail to written mail
b) They are away from home and unable to receive correspondence
c) Their home circumstances make it undesirable for them to receive letters
d) They wish to receive correspondence, including diagnostic testing results, appointment letters, or copies of hospital correspondence without the delay of written mail

However, if you allow an eMail to disclose personal data, YOU could personally fall foul of the Data Protection Act 1998. The Data Protection Principle 7 is clear:

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

Guidance on how to ensure compliance with the Data Protection Act whilst eMailing service users are presented in Appendix F.

10 MANAGING E - MAILS AS TRUST RECORDS

Many staff regard eMail as a highly personal form of communication, with little or nothing to do with record keeping. However, when eMail messages contain evidence of business decisions, actions and transactions they become records, which are subject to the same legal requirements, restrictions and standards as any other corporate record produced in any form or media by the Trust.

Electronic messages sent or received in the course of business transactions are Trust records and must be retained for as long as they are needed for Trust organisational and legal requirements.

When eMails contain information about business activities, like records in other formats, they are subject to legislation such as the Public Records Act (1958 & 1967) the Data Protection Act (1998), the Freedom of Information Act (2000) and the European Convention on Human Rights and as such are subject to legal processes.

Records communicated using eMail need to be identified, managed, protected and retained for as long as they are needed to meet operational, legal, audit, research and other requirements.

All members of staff are responsible for identifying and managing any eMail messages that constitute a record of their own work. When eMail is sent or received a decision needs to be made about whether that eMail needs to be captured as a record.

Where a group of staff are working on a project one person should be nominated as main archivist to ensure a complete record of any decision making process is retained, this is especially significant in respect of any contractual negotiations.

An **eMail message can be a record** if: -

- It contains a specific piece of information produced or received in the initiation, conduct or completion of Trust business, and can offer sufficient content, context and structure to provide evidence of such activity.

In order to clarify which eMails should be treated as records the following guidelines should apply. eMails that meet one of the following criteria should be regarded as records of business activity: -

- Were developed in preparing reports, papers, studies
- Reflect official actions taken
- Convey information on programmes, policies, decisions
- Convey statements of official policy or rationale for official decisions
- Document oral exchanges where official policy/decisions were discussed
- Have legal and/or financial import for the Trust

All members of staff must be able to identify which of their eMail messages should be captured as a record of their work. This is likely to have greatest impact on senior staff across the Trust.

As the types of records produced by the Trust can be diverse it will be necessary for line managers to work closely with staff to provide more specific guidance in different functional work areas about which eMail messages will constitute records of business activity

As eMail messages can be sent to multiple recipients there are specific guidelines to indicate who is responsible for identifying and capturing an eMail as a record:

- For internal eMail messages, the SENDER of an eMail message, or INITIATOR of an eMail dialogue that forms a string of eMail messages
- For messages sent externally, the SENDER of the eMail message
- For external messages received by one person, the RECIPIENT
- For external messages received by more than more person, the person responsible for the area of work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

When an eMail message has been identified as a record of a business transaction it is important that the message is retained with other records relating to that particular business activity.

This will mean moving the eMail from an individual's mailbox and putting it in the appointed records management system used by the individual / department /Trust.

This can be a hierarchical list of subject folders on a shared drive, a paper file, or an electronic document and records management system.

Retention is then governed by the retention and disposal schedule of the associated file series, determined as part of the Records Management Policy of the Trust. (Retention schedules and the Trust's Records Management Policy will be available as part of the Information Governance Knowledge Base on the Trust's intranet.

In order to function effectively as a record, eMail messages need to retain their content, their structure, and the business context in which they occurred.

For example it is important that the following header information is captured and permanently recorded (in an unalterable state) along with the message:

- The senders eMail name and address
- The recipients eMail name and address
- Names and addresses of any additional recipients
- Date/time of transmission and receipt

Further advice and guidance can be obtained from the IM&T Department.

SECTION 2 IM&T POLICIES

2C INTERNET USAGE

1. Purpose

Access to the Internet is primarily provided to enable staff to access information and services to support them in the execution of their duties.

The Trust considers the Internet as an important means of communication and recognises the importance of proper Internet content and speedy replies in conveying a professional image and delivering good patient care service.

Whilst it is acknowledged that some personal use of the Internet system is inevitable non-work related use during normal working hours is not encouraged and staff must not abuse that facility. All Internet access generated from within the SCAS service carries information which clearly identifies the organisation as being a point of origin.

This Internet usage policy states the position of the Trust and sets out the obligations that all members of staff have when accessing and using the Internet, with special regard to the protection of confidentiality, integrity and availability of the Internet system. This policy is designed to protect the Trust and individuals.

2 IT FRAMEWORK AND CONTROLS

2.1 Core Principles

2.1..1 All identified Trust staff will have access to Internet facilities using personally identifiable accounts. The level of access will be as requested and authorised by Managers in accordance with this policy.

2.1..2 Authorisation levels will be appropriate to the role and position of each individual user. Any variations to this will only be made with the explicit consent of the Associate Director of IM&T or the Head of ICT, and will be reported to the Information Governance Group

2.1..3 Personal use of the facilities will be allowed within the confines of this policy framework so long as this does not interfere with work

2.1..4 Safeguards will be established to protect the security, integrity and availability of the Trust's systems. These are covered within the Trusts Anti-Virus policy (*IM&T Policy 2E Version 004.02 January 2017*)

2.1..5 The requirements of the relevant Acts of Parliament and mandatory national policies will be observed at all times.

2.1..6 Staff awareness of copyright and contractual issues will be raised.

2.1..7 Guidance on Internet usage provided in this policy

2.1..8 Guidance on housekeeping to ensure efficiency in the operation of the network and personal folders is provided in this policy.

2.2 Risks associated with the use of the Internet

The very nature of the Internet means that there are a number of potential risks to the individual and the Trust associated with its use.

For example

- Information can be accessed from a variety of sources, sometimes these may not be authorised or legitimate, and the accuracy of data may be brought into question.
- Information, photographs, software, music or video downloads may be subject to copyright; individuals downloading such material may inadvertently create legal and operational issues

for the organisation through their actions if they do not have the author or owner's permission to do so.

- Downloaded items can contain computer viruses, which are particularly damaging to the Trust's computer systems.
- There are numerous illegal, illicit and mischievous Internet users who can dupe users into accessing their sites for personal gain. .
- Accessing authorisation pages on third party websites can legally bind the Trust contractually in certain circumstances without proper authority being obtained internally.
- Not all information available from the Internet is business specific. It is relatively easy to find, or come across, sites containing pornographic or illegal material.
- Internet use can be addictive, and time consuming.

2.3. IT Controls

2.3.1 There are a number of safeguards and controls built into the Internet service provision to protect it from overload, restrict access to known non-work related sites and ensure fair, appropriate and consistent use by all staff across the organisation. These safeguards and controls are also dependent on good user practices and housekeeping measures.

2.3.2 A detailed list of restricted sites will be reviewed annually by the Information Governance group. Any individual amendments to the list will only be granted with the explicit approval of the SIRO, Associate Director of IM&T or the Head of ICT and will be reported to the first available IM&T Control Board meeting as an Exception.

2.3.3 The Trust will deploy effective Firewall and Anti-Virus solutions across its ICT Infrastructure. These solutions will be subject to regular external Audit review, with the findings given to the Trusts Audit Committee and the Executive Group. The specific details of the solutions deployed will not be routinely detailed in any published or publicly available documents (hard copy or web based), but will be advised as appropriate to the Trust Board, its Audit Committee and the Executive Group.

2.3.4 Access to any personal e-Mail account that does not have an nhs.uk identifier should be avoided (This includes all commercial and freely available sites including but not restricted to MSN, Hotmail, Googlemail, BT, Tiscali, AOL etc.) as it is not possible to easily control downloads of non-work related material, or quarantine potential viral infections from these locations. Where possible such facilities will be routinely blocked but it is the responsibility of individual users not to breach this restriction.

2.3.5 At all times ICT staff will put protection of the corporate infrastructure at the heart of any and all decisions relating to access to, or downloads from, Internet locations.

Any exceptions to these controls MUST be approved by the SIRO, Associate Director of IM&T, or in their absence a Head of ICT. Exceptions will be reviewed by the IM&T Control Board and as appropriate included within standard operating routines or removed.

2.4. Personal Use

2.4.1 Limited personal use of corporate Internet facilities is currently permitted provided that full compliance with this policy is maintained. Employees should regard this facility as a privilege that should normally be exercised in their own time without detriment to the job and not abused.

2.4.2 Inappropriate or excessive use **WILL** result in disciplinary action and/or removal of facilities. Staff should be aware that use of the Internet might be subject to monitoring, and disclosure

to others. In order to respect and protect the privacy of individuals in compliance with the European Convention on Human Rights it is strongly recommended that personal use of the Internet does not contradict the ethos of common decency or adversely impact on the working or social lives of others.

2.4.3 Staff are not encouraged to use the corporate network for personal shopping, banking or trading as we cannot guarantee the confidentiality of any information processed, including details of credit cards or personal accounts which are recorded on devices which are for shared use. Use of personal bank credit or debit cards contains a level of risk to the individual and the Trust will not be held accountable for any instances where such information is subsequently misused.

3 USE OF INTERNET FACILITIES

3.1 Unacceptable Internet Usage

3.1.1 Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

3.1.2 Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.

3.1.3 Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.

3.1.4 Creating or transmitting "junk-mail" or "spam". This means unsolicited commercial webmail, chain letters or advertisements.

3.1.5 Using the Internet to conduct private or freelance business for any purpose whilst working.

3.1.6 Creating, downloading or transmitting data or material for the purpose of corrupting or destroying other user's data or hardware.

3.1.7 Downloading or streaming video or audio for personal entertainment purposes.

3.1.8 Use of corporate networked PC's to access "Social Networking" and data sharing sites such as Facebook, Twitter, Snapchat or YouTube for non-work related purposes should be limited to non-working time and only with the approval of line managers. Whilst such sites can also be accessed by members of staff in their own time, using their own equipment (PC/laptop/mobile phone, PDA etc.) the Trusts policies in respect of harassment or bullying can still be applied should derogatory comments be made in respect of other staff members or the organisation and will be dealt with in accordance with existing trust disciplinary procedures..

3.2 System Monitoring

3.2.1 Internet traffic is monitored automatically (each site a user visits is noted, showing times and pages viewed) to ensure that damaging code or viruses do not enter the organisation's network or systems. The organisation also uses software that can prevent users visiting sites that may contain illegal or pornographic material. These logs are audited periodically by IM&T staff and any repeated attempts to access unauthorised sites can be reported to relevant line managers and Directors for further investigation.

3.2.2 If there is evidence that a user is not adhering to the guidelines set out in this policy, the Trust reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action. This includes action against anyone found to have changed PC settings to modify corporate "proxy" access allowing them to temporarily bypass Trust protective measures. Only authorised ICT staff have permission to make such changes

The corporate system should not be used for personal access to non-work related social networking sites such as "Facebook"", YouTube", "Snapchat" etc. during normal working time. Any member of staff found to be accessing such a site without authorisation when they should be working may find

themselves subject to disciplinary procedures. Disciplinary action may also be taken in respect of any derogatory, defamatory or offensive remarks posted by staff on any website, public forum or chat room. Where such comments are made regarding another individual they may be considered as harassment and bullying and dealt with accordingly under the trusts relevant HR Policies.

Compliance with all Trust policies is a condition of employment and a breach of policy may result in disciplinary action. This policy is complementary to other Trust policies and protocols and should be used in conjunction with them, but especially with the

- Data Protection policy
- Confidentiality code of conduct
- Freedom of Information policy
- NHS Information Security and Management guidelines
- Network Security and Access Control policy.

Guidance on Internet usage is provided in Appendix G and H

SECTION 2 IM&T POLICIES

2D NETWORK SECURITY

NEW POLICY IN DEVELOPMENT

SECTION 2 IM&T POLICIES

2E ANTI VIRUS

1 Purpose

This policy applies to the use of all ICT equipment in use within South Central Ambulance Service NHS Foundation Trust (SCAS). It sets the standards for the deployment of antivirus software, states the position of the Trust and sets out the obligations that all members of staff have in ensuring the security and stability of the corporate infrastructure. This policy is designed to protect the Trust and individuals.

2 Computer viruses

Computer "viruses" are malicious programs which can be unwittingly copied between computer systems. Their effect is to damage, destroy or prevent access to data. The most common way for a virus to infiltrate a system is by the introduction of an "infected" data stick or SD card, or infected files downloaded via the Internet or e-Mail. Other devices can become infected through use on an affected system.

Though the Trust deploys software that can assess downloaded files to check that they are virus free it is the responsibility of each individual user to ensure that this is done on files or media that they are accessing or using.

3 Virus on networks

Networked systems are particularly susceptible to the spread of viruses once introduced. For this reason SCAS takes Network Security very seriously. The corporate network infrastructure is connected to NHSnet and its own Virtual Private Networking infrastructure via Firewalls, which provide some protection by filtering traffic according to source, destination and type of message.

Strict rules are in place to ensure that all connections via the Firewall are legitimate and authorised by the Associate Director of IM&T or the Head of IT. The rules and connections are reviewed annually by the Trusts IM&T Control Board.

Anti-virus software is installed on all SCAS servers. The actual software will be approved by the Trusts IM&T Control Board following recommendation from the Associate Director of IM&T The name of the software, or the manufacturer will not be disclosed in writing, or verbally, without the express permission of the Associate Director of IM&T to any third party to better protect network security.

The Associate Director of IM&T or the Head of IT must authorise the connection of any workstation to the corporate Infrastructure.

All devices operating on the network will employ resident virus check and removal programs, these may be resident to the individual device or distributed from within the infrastructure.

It will be considered a disciplinary offence for any member of staff to knowingly bypass this software, or ignore any warning messages that might be given.

4 PRECAUTIONS

4.1 Anti-virus precautions

All computer systems connected to the SCAS infrastructure will have disk-resident virus check programs as approved by the Associate Director of IM&T and the Trusts IM&T Control Board. Anti-Virus software must only be installed and configured by IT Services. Users must not disable or interfere with anti-virus software installed on any computer.

All Trust servers must be regularly updated in respect of Anti-Virus and other supplier security patches. Arrangements will be made by IT with relevant departments and system suppliers to ensure that this is achieved, or where a supplier cannot approve the relevant update that other arrangements are put in place to protect the system and the overall infrastructure.

Only equipment that is owned or provided by the Trust can be connected to the Trust network. Connecting any other equipment, including mobile telephones/organisers, data sticks, cameras, iPads, tablets or personal laptops is strictly prohibited. Data sticks, cards and diskettes are not routinely approved for use on the Corporate ICT equipment. The Associate Director of IM&T will agree with relevant directors and service leads any exceptions. Where approval is given responsibility for ensuring that they are used safely and securely will reside with the relevant line managers and users themselves

Only encrypted data sticks sourced from the SCAS IT department will be approved for use. Any data sticks authorised for use by trust staff will require that the data transferred to them is encrypted. The trust will deploy as a minimum standard NHS approved encryption protocols. Individuals provided with such data sticks will be responsible for routinely checking them prior to use to ensure that they do not contain viruses or other unwanted attachments.

New software applications must only be installed by staff or suppliers approved by the Associate Director of IM&T or the Head of IT. All such applications will be checked to ensure that they are virus free, and that they are legitimately licenced for use on SCAS equipment. Any instances of unlicensed software will be disabled without consultation, and further access will not be permitted without the express authorisation of the Associate Director of IM&T.

No software programs, applications or executable files should be downloaded from the Internet and installed onto a PC without the specific consent of the Associate Director of IM&T or the Head of IT. Unauthorised downloading of software may breach the copyright licence, could introduce a computer virus to the system, and is a breach of the Trusts Internet Policy

4.2 Failure to take precautions

It should be noted that it is a criminal offence under the Computer Misuse Act 1990 to deliberately introduce a virus to a computer system. It shall be a disciplinary offence to introduce a virus to any SCAS computer systems by failing to observe the precautions noted above.

5 VIRUS CONTROL

5.1 Checking for a virus

Master copies of media containing important data or program files should be write protected where possible. All line managers are responsible in ensuring that proper precautions as detailed above in para 4.1 are taken when staff are using data sticks, cards, external disk drives or downloaded files.

When a data stick is issued it will be virus free, it should be recorded appropriately. The record should stipulate the following information:-

- Data stick identifier
- date anti-virus check was made
- version number of the anti-virus software used
- signature and initials of the person carrying out the check

It is the responsibility of the individual user to ensure that the Data stick is rechecked at any time after they have been used on a non-SCAS device.

5.2 When a virus is found

Where a disk, data stick, card or computer is found to be infected with a virus, the following will apply:-

5.2.1 The ICT Helpdesk will be informed immediately that a virus has been discovered. IT support will then either arrange to attend and deal with the virus OR will confirm with the individual concerned procedures to quarantine or clean the infected disk or computer using the provided Anti-Virus software.

5.2.2 If a data stick or disk is successfully cleaned, a label shall be affixed clarifying that the device has been scanned and is now clean. Where it is not possible to clean the infected device, it shall be clearly marked "VIRUS INFECTED" and given to the relevant ICT team who will contact the manufacturers of the anti-virus software for further advice in an attempt to isolate and remove the virus. If the IT Department cannot safely eradicate the virus, the disk or data stick will be physically destroyed. There will be no exceptions to this procedure.

5.2.3 The Department Head will be informed in writing that a virus has being detected and measures will be taken to virus test computers and electronic media within that department. Where a computer is suspected to be infected, the computer should be disconnected from the network if attached. The ICT Department keep a log of all computer systems and electronic media checked, also a log will be kept of all virus detected within the SCAS, and action taken to eradicate infections and educate the user.

5.3 Previous Backups

Where a virus is introduced on to a main server within the SCAS infrastructure, the infected server will be immediately disconnected from the network. The infected server will be cleaned and checked to ensure that previous backups taken are not affected before the system is brought back into active use, utilising the most recent “clean” back up available

5.4 Working Remotely

Staff working away from Trust office locations must ensure that they use the anti-virus facilities resident to their laptops to ensure that any approved data sticks or diskettes are checked prior to being loaded, as well as checking any items downloaded from the Internet.

In the event that they do detect a virus then the infected product must be removed from the Trust equipment and nothing should be downloaded from the disk or data stick. The ICT Service desk should be contacted at the earliest opportunity and arrangements made to have the media and/or laptop inspected by ICT staff to ensure that no infection has taken place before the portable computer is re-connected to the SCAS internal network or electronic media are loaded on to SCAS’s computers.

SECTION 2 IM&T POLICIES

2F CYBER SECURITY

NEW POLICY IN DEVELOPMENT

SECTION 2 IM&T POLICIES

2G MOBILE DEVICE USAGE

NEW POLICY IN DEVELOPMENT

Security of Mobile Devices

All staff provided with mobile ICT equipment, including but not restricted to, laptops, mobile telephones, BlackBerry's and tablet devices are responsible for the safe keeping of such equipment both in and out of work.

All laptops are required to be fully encrypted. Other mobile devices must be encrypted or protected by other such data security features.

Extra care of equipment must be taken when away from the normal place of work – including when travelling to and from home or to other locations for work related purposes.

When travelling by car equipment that is not in use should be secured out of sight, preferably in the car boot, and should not be left in the car when the journey ends, or is broken.

It is recommended that laptops should be removed from cars at the earliest opportunity, including occasions where journeys home are broken for shopping or social purposes. It is a requirement that no ICT equipment is left in cars or other vehicles overnight if the vehicle is not garaged on a Trust site – and only then if there is a staff presence. On no account should equipment be left in a car outside an employee's home or temporary accommodation (e.g. hotel or educational establishment).

Any failure to protect Trust equipment through failing to follow this advice results in the loss of equipment will be dealt with under the trusts disciplinary procedure as misconduct, or should the loss also include the loss of confidential or patient related material, gross misconduct.

SECTION 2 IM&T POLICIES

2Z INCIDENT REPORTING

PURPOSE

South Central Ambulance Service NHS Foundation Trust (SCAS) Security Policy requires that a system for reporting and responding to Security incidents exists. This is to ensure that any breaches of security are detected, reported and investigated in an efficient and effective manner, and that the damage from any such incidents is minimised. It is the responsibility of all staff to ensure that any incidents are reported as described in this procedure. This document relates to ICT related issues.

1.1 The Importance of Reporting Incidents

The majority of IT security breaches are innocent and unintentional and will therefore not normally result in any form of disciplinary action. By reporting them you will help the ICT Team to improve data security and raise awareness as to how these incidents can be avoided in the future. Where major data security breaches occur or other incidents which contravene SCAS IM&T Policies and procedures are detected, then in some cases disciplinary action will be taken.

1.2 Definition of an Incident

An IM&T security incident is defined as any event which has resulted, or could result, in:

- The disclosure of confidential information to any unauthorised individual.
- The integrity of a system or data being put at risk.
- The availability of the system or data being put at risk
- An adverse impact

Examples of type of incidents are included in **Appendix I.**

2. Incident Reporting

All incidents or information indicating a suspected or actual security breach must be reported as soon as possible to your immediate line manager and a Head of IT or the Information Governance Manager. If you wish to report an incident directly to the Director of Finance as Corporate Senior Information Risk Owner (SIRO) or the Associate Director of IM&T then you may do so – they will inform the Information Governance Manager in all cases where a breach exists.

Should you consider the breach to involve a senior ICT or IM&T officer in some way, then the incident must be reported directly to the Associate Director of IM&T, the SIRO or the Chief Executive. All reports received will be treated in strict confidence, including "false alarms".

3. SCAS Security Management Responsibilities

In the absence of a formal Security Manager role within the SCAS IM&T or Information Governance structures then responsibility for the role is devolved within the IM&T structure. These responsibilities include;

- Opening an Incident Form for all incidents reported using the Trusts standard Incident Report Form (**IR1**) using the Trusts Datix reporting system.

- Investigating and documenting incidents on the Incident Form

- Classifying the incident as soon as possible (reclassifying if necessary as the investigation develops), and maintaining a log of all Incident Forms

- If appropriate, reporting all major or acute incidents to the Associate Director of IM&T, Executive Management Team and the Chief Executive immediately

- Reporting any incidents which could involve the NHS-wide network to the relevant Officer in NHS England

- Monitoring "usual" incidents - those incidents which occur primarily as a result of human error (Wrong passwords or User Id's being entered, Passwords not being changed when time expired etc.). This monitoring to be achieved through quarterly reviews of relevant files and service desk records.

- Producing a quarterly report of Unusual Incidents and a summary of trends in usual Incidents for the Information Governance Group.

- The Associate Director of IM&T will regularly report to the Trust's Audit Committee on all matters relating to ICT security and management, including updates from the quarterly reports and trend analyses.

IM&T POLICIES APPENDIX A

IM&T DEFINITIONS

For the scope of these policies the following definitions apply:

Apps	an abbreviation for “applications” is a piece of software which can run on an electronic device
Custodian	normally a service provider who has local management responsibility for the security of the information that resides upon or passes through their service. They have not necessarily created the information nor used it. An example of a Custodian is the manager of an IT system. An Owner can delegate certain responsibilities to a Custodian.
Electronic Media	any magnetic od electronic device which can be used to record and store data for use on a personal computer
Information	knowledge which can be transferred or stored in a number of forms. These include documents, telephone and face to face conversations, faxes, data in computers and data transmitted between computers or to computer peripherals.
Internet	a general term that covers access to numerous computers and computer systems worldwide that are accessed electronically. Such systems include the World Wide Web (WWW), e-Mail (dealt with in a separate policy), File Transfer Protocol (FTP), newsgroups, Gopher, etc. The Trust uses secure network services, including NHSnet and its own Virtual Private Network (VPN) to access these systems.
Owner	anyone who has managerial responsibility for the creation of Information or reception of Information from Patients and other external parties is normally the Owner. The Owner is responsible for the security of such information. A third party Owner may delegate SCAS to transcribe information (for example to a typist) but will always retain the core responsibilities of ownership. Ownership can be inherited as a result of an organisational change or job move.
Personal Computer	any one of the following; desktop computer, laptop, tablet, hand held device, smart phone
Risk Management	the identification, measurement and cost effective control of risks which threaten the assets and/or earnings of an enterprise. Reference should be made to the organisations Information Security Policy and to a standard risk assessment methodology.
Software	as a computer program that is designed to carry out specific functions
User	anyone who receives, stores, manipulates or forwards information. A User may delegate SCAS to deal with received information (for example to a secretary who in turn becomes another user. Owners and Custodians can also be Users.
Virus	a self-replicating piece of software, which may cause damage to the operating system of the computer, the storage devices, and any data and/or software stored on them.

IM&T POLICIES APPENDIX B

eMail ETIQUETTE: Do's and Don'ts

This fact sheet is intended to complement the Trust's policy on eMail and give a reminder about some useful Do's and Don'ts.

DO

1. Be aware of and comply with the Trust's policy on the use of eMail at all times.
2. Remember that all eMails within the corporate infrastructure are the property of the Trust.
3. Understand that eMail messages are as legally binding as any other form of written communication
4. Exercise the same degree of care and professionalism in regard to the content of an eMail as you would with a letter.
5. Be aware that all eMails sent or received by the Trust are subject to both the Data Protection and Freedom of Information Acts and may be disclosed to a third party.
6. Make sure that your eMails always contain appropriate contact information – set up automatic signatures to do this – new mail or first time responses should include job title, telephone numbers and location address, this can be reduced to telephone numbers in other replies.
7. Remember the basics of business writing, the need for accuracy, professional standards and common courtesy.
8. Always fill in the subject line with meaningful, descriptive and appropriate text.
9. Send messages only to relevant people and be specific about whether action is required or not.
10. Read and reply to eMail messages frequently – once a day as a minimum if possible.
11. If absent from work leave an "Out of Office" message or make alternative arrangements for your eMails to be dealt with during your absence.
12. Use shared drives, or intranet rather than sending a large attachment.
13. Keep your mail box tidy
    - delete unwanted eMails as soon as they are no longer required.
    - set up a separate folder for your personal eMails.
    - set up folders for eMails that you want to store for short term use
    - store those eMails that contain records of business activity outside of the eMail system in your normal electronic filing system
    - restrict manual record keeping to a minimum
14. Understand the eMail implications of home working.
15. Remember that eMail (particularly outside of NHS.net) is not a secure form of communication.
16. Mark personal and private eMails as such and do not store in mailboxes.
17. Be aware of the Trusts related policies on
    - Data Protection
    - Confidentiality Policy
    - Freedom of Information Policy
    - Information Security Policies
    - Records Management Policy.

DO NOT

1. Use SCAS addressed eMails for personal gain or profit.
2. Use your eMail to represent yourself as someone else.
3. share passwords with anyone, as they will then be able to send eMail under that name. YOU are personally liable for any misuse logged under your username and password.

4. Use eMail to communicate confidential, sensitive or potentially embarrassing information.
5. Use eMail to communicate to patients unless you follow the Trust's protocol.
6. Post messages that contain political views, with the exception of those permitted for trade union use.
7. Advertise or otherwise support unapproved or illegal activities.
8. Provide lists or information about Trust employees to others.
9. Use your eMail in-box as your personal filing system – remember read – action – delete.
10. Use your eMail system to store Trust Records – these need to be moved out of the eMail system and into your normal filing system (preferably electronic or paper).
11. Allow backlogs of unwanted eMails to accumulate in your mailbox.
12. Send eMails to Trust wide groups unless it is absolutely necessary – do not include large attachments with these eMails – put the documents and information on the intranet instead.
13. Do not reply to "all" unless it is appropriate
14. Send eMails that contain libellous, offensive, racist, defamatory, obscene or pornographic remarks, pictures including personal items for sale, or sponsorship requests.
15. Send or forward any eMail that contains advertising materials, chain letters, jokes and executables or junk mail of any kind.
16. Use eMail to gossip or let off steam.
17. Mix personal and work eMails.
18. Address more than one topic in any one eMail if it can be avoided – particularly when writing to a group, some members of which may not be involved in all the matters you want to communicate.
19. Annotate or change the text of the original eMail when replying to it without making this clear in the message that you send.
20. Send any files or eMails containing person identifiable information to your home account.
21. Use a non-Trust eMail account for Trust business (unless specifically authorised to do so through the Trust's Home Working and Mobile Devices Policy.

IM&T POLICIES APPENDIX C

eMail : GOOD HOUSEKEEPING

It is the responsibility of all individuals to manage their mailboxes appropriately and to ensure that their use of the eMail messaging system does not compromise the ability of others to effectively do so.

It is vital to undertake a number of "good housekeeping" routines on a regular basis ensuring that eMails are actioned, deleted or stored for short term reference purposes in personal folders, or moved to a more permanent file location if they are records of corporate business activity.

1. Check your eMail inbox on a regular basis – at least once every working day where possible.

2. Delete junk mail immediately or add to the Junk Senders list.

3. Reply to messages addressed to you as soon as possible – if only to acknowledge receipt of the message.

4. Keep the amount of mail in your mailbox (including Inbox, Sent Items, and Deleted Items) to a minimum – this will make your mailbox easier to manage and will conserve space.

5. Delete all unwanted messages and messages that have been dealt with, from your inbox to your deleted items box on a regular and on-going basis.

6. To ensure that items are actually deleted from the system you also need to delete all items from your deleted items box on a regular basis – right click on the deleted items icon and "empty deleted items folder". It is unacceptable practice to use the deleted items area for storage. The default setting which IM&T install on all accounts is that the "Deleted Items" folder is emptied every time a user closes their Outlook session.

7. For those eMails that you wish to keep for short term (i.e. 2-6 months) reference purposes transfer to personal folders

8. Develop an orderly filing system within personal folders, which works for you. Review these saved messages on a monthly basis. Ensure that there are no eMails within your Outlook folders that are over six months old.

9. EMails which can be identified as corporate records need to be retained and transferred out of the eMail system and kept in the appointed records management system used by the individual or department.

10. If you need to keep Attachments (documents, spread sheets etc.) save them outside of the eMail system e.g. within your normal electronic filing system

11. Think about procedures for when you are away – use the Out of Office Assistant - or provide mailbox access to a delegated and trusted third party.

12. Contact the ICT Service Desk to report any incidents or breaches in security in relation to any wrongly addressed eMails containing patient or personal information or data.

IM&T POLICIES APPENDIX D

eMail : SPAM AND PHISHING – HINTS & TIPS

This fact sheet is intended to complement the Trust's policy on e-Mail and give some simple guidance on how best to minimise the threat and distraction of Spam mail or Phishing

Definitions

Spam

Electronic junk mail, or junk newsgroup postings. Generally e-Mail advertising for some product, but potentially a mechanism for distributing viruses and other computer related invasive attachments.

Phishing

The act of sending an e-Mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Tips

- You will usually start to receive spam if you give out your Trust e-Mail address to websites. This information is usually passed onto other companies and their advertising then subsequently targets you.
- Some spam e-Mails offer you the choice to opt-out of receiving these types of emails. Although this seems a good idea, it just confirms to the sender that the email address they are sending to is live and more spam may be sent.
- Forward a copy of the spam message you are receiving to the ICT Help Desk who will attempt to prevent future delivery based on a set of rules and keywords
- Do not give out your Trust e-Mail address on forms or websites or in newsgroups unless absolutely necessary, as part of your official duties.
- Do not reply or try to unsubscribe.
- Do delete the message or setup a junk mail rule to delete this type of message.
- Identifying scam e-Mails (Phishing)
  - Scam e-Mails often state in the subject and in the e-Mail that you need to update or confirm your personal details.
  - Scam e-Mails pretend the page they send you is secure or an Online Banking page.
  - Scam e-Mails aren't normally addressed to you by name, as they don't generally know any of your details other than your email address.
  - Spelling mistakes in the e-Mail and the presence of an IP address in a web link are both clues that the email is a bank phishing attempt.
  - Another giveaway is the lack of a personal greeting, although the presence of personal details is not a guarantee of legitimacy.

For more advice see

http://www.companieshouse.gov.uk/securityAdvice/index.shtml

IM&T POLICIES APPENDIX E

eMail Etiquette: GUIDELINES FOR WRITING

The Trust's Executive Board is supporting a number of simple steps which are designed of improve the effectiveness and efficiency of our eMail use.

The Subject Line

All eMails should utilise the following prefixes on the subject line:

- **ACTION** : for mails where you want the recipient to do something – if the whole action can be wrapped up in a short sentence within the subject then end it with (EOM) to show that it's the end of the message
- **INFORMATION** : for mails where you want the recipient to be aware of something without them necessarily needing to respond… the equivalent of using CC when asking someone else to do something.
- **RESPONSE**: when replying to an action request.
- **URGENT** : before any of the above prefix' where appropriate (we are defining "appropriate" as relating to actions that if not delivered could threaten or jeopardise the delivery of a major strategic or corporate priority for the Trust that are needed within the next two days) adding a due date/time at the end of the subject line.
- Following the prefix the subject line should give a clear indication of the emails content, which also helps future retrieval of messages.
- Outlook includes tools which let you indicate if the subject matter is sensitive, whether it is of high or low importance, and whether you have set a deadline for response.

Subject and Tone

- Greet people by name at the beginning of an e-mail message - REMEMBER – maintain the conventions normally used in traditional communications
- Identify yourself at the beginning of the message when contacting someone for the first time
- Ensure that the purpose and content of the e-mail message is clearly explained
- Please ensure that your signature lines include relevant contact details – even when you reduce your "reply" signature to just your stylised name it is also effective if you can include contact details such as mobile or desk telephone number on the same line – new eMails should always include your full contact details including postal address and job title.
- Ensure that the email is polite and courteous
- Make a clear distinction between fact and opinion
- Proof read and spell check messages before they are sent to check for errors
- Try to limit e-mail messages to one subject per message
- Include the original e-mail message when sending a reply to provide a context - however where there are multiple responses to an original message consider deleting older mails (the "tail")

- Where the subject of a string of e-mail messages has significantly changed start a new e-mail message, copying relevant sections from the previous string.
- Ensure e-mail messages are not unnecessarily long
- Ensure that attachments are not longer versions of e-mails
- Summarise the content of attachments in the main body of the e-mail message

Structure and Grammar

- Use plain English
- Use paragraphs to structure information in the same way that you would if you were writing a report
- Put important information at the beginning of the e-mail message
- Avoid using abbreviations
- Avoid using CAPITALS. The use of capitals makes people think you are shouting at them.
- Conversely don't use all lower case because it's hard to read
- Try not to over use bold or italic text
- The use of internet abbreviations, characters and symbols such as ☺ is not encouraged

Addressing

- Distribute e-mail messages only to the people who need to know the information
- Using 'reply all' will send the reply to everyone included in the original e-mail. Think carefully before using 'reply all' as it is unlikely that everyone included will need to know your reply.
- Use the 'To' field for people who are required to take further action and the 'cc' field for people who are included for information only.
- Think carefully about who should be included in the 'cc' field
- Ensure the e-mail message is correctly addressed

General

- Try not to overload the e-mail system – Think about the appropriateness of use and other ways of communicating and information sharing. Use the Trust's intranet site wherever possible.
- It is better to respond in due course, and calmly, than immediately in anger…

CHECKING your eMails at set times during the day allows you to control their impact, as opposed to being constantly distracted as they arrive and you're working on something else – perhaps either end of the day and just before lunch.

THE TWO MINUTE RULE – if an eMail takes less than two minutes to read and respond to then deal with it immediately even if it's not high priority as it's been proven that it takes longer if you read, store and pick up later.

FILTER YOUR CC'S – if messages are only FYI or you're being told something to "keep you in the loop" then filter them to a "Read Later" file so that they do not interrupt your day, if you find later that someone has actually expected you to do something in a mail that you've been cc'd in tell them so that they don't make the mistake again.

CLEARING YOUR INBOX – one simple mechanism that can improve the flow of work is to filter read eMail into broad areas such as "Action Items", "Waiting", "Reference" and "Archive" which

you can then sub-divide into relevant projects or work areas -this does make searching for specific mails simpler.

NON ESSENTIAL MAIL - we all receive newsletters, supplier information and other "junk mail" that evades the main filtering systems... you can easily filter these out of your inbox into whatever sub groups you wish.

MANAGE YOUR DELETIONS – please don't be afraid to delete old mails, especially where you've replied or there's a longer chain developing...we only have limited space available in our mail boxes- our corporate policy supporting Freedom of Information and Data Protection requirements states that we only retain six months of data in our mail system... if something is needed to be filed for longer term use it should be elsewhere within our system NOT in eMail archives... if you follow policy and retain only six months of eMails then the task is much easier. Main file storage can be readily shared as necessary and is much more effective than closed mail box accounts!

Finally we can all help each other by ensuring that we follow some simple etiquette when composing and responding to eMails... ensure that they are succinct but relevant... one or two paragraphs that include the relevant facts are better than screen loads of waffle. Only send mails to the people that need to get them... and when replying be careful about replying to all... usually it is only the author that you need to reply to.

IM&T POLICIES APPENDIX F

eMail : COMMUNICATIONS WITH SERVICE USERS

E-ail outside the NHS net is an insecure method of communicating, and confidentiality cannot be guaranteed. Service users across the NHS are however increasingly requesting e-mail correspondence for a variety of different reasons.

- They simply prefer e-mail to written mail
- They are away from home and unable to receive correspondence
- Their home circumstances make it undesirable for them to receive correspondence
- They wish to receive correspondence, including diagnostic testing results, appointment letters, or copies of hospital correspondence without the delay of written mail

If you allow an e-mail to disclose personal data, YOU could personally fall foul of the Data Protection Act 1998. The Data Protection Principle 7 is clear:

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

It is important to follow the correct procedure

1. The patient MUST provide written authorisation that e-mail communication is appropriate. (In some cases such as extreme weather or disruption to mail services this may not be practical so ensure that you document these situations.).

   Check that the name spelling is consistent with the name in the patient notes.

   Show the patient the written e-mail address, and ask them for written authorisation to use e-mail. Record any limits on e-mail use such as:
   - E-mail only, do not send correspondence
   - E-mail only until 31 August, when patient returns from holiday, or
   - E-mail appointments only, not clinical information, or
   - E-mail blood test results only, or
   - Send written letter as well as e-mail.

2. The patient MUST provide a **personal e-mail address**.
   Group e-mail addresses do not comply with the Data Protection Act and as such must not be used e.g.

   thesmithfamily@email.service, or

   johnandmarysmith@email.service or

   enquiries@smith.industries

3. All outgoing and incoming patient e-mails MUST be added to the patient notes.
4. If a paper copy of the same document would normally go into the patient notes, or be forwarded to another hospital or health centre, then ensure that this is done.
5. Explain the risks of using e-mail to the patient – see Section 4.2
6. Ensure that the e-mail is ALWAYS sent from an NHS-net system. Non-NHS use, such as an academic or private message, may wrongly give the impression that the e-mail is an official NHS message. In addition if the sender does not appear to be an NHS source, the patient may delete it as spam.
7. In the subject line, use a neutral description that does not disclose sensitive information.
8. As e-mails are insecure, they should only contain the minimum necessary information.
9. Attachments can be used to transmit other files, including MRI or X-ray images, or pathology result graphs. However some e-mail systems block attachments of any size or of a certain minimum size. *It is therefore good etiquette to send a preliminary e-mail to tell the patient that a second message will follow with an attachment.*
10. If the patient has not used e-mail personally, but asks a relative to do this, then this is acceptable only when a known carer is involved in the treatment plan.
11. Consider using a department e-mail address as the sender rather than individual staff names.
12. Remember that it is vital your e-mail goes to the correct recipient – carefully check first name, surname, NHS number, etc. where necessary before sending.
13. If a patient requests that informal e-mail correspondence be omitted from their paper notes then the Data Protection Act allows this and provides for e-mails or any other data to be excluded from the care record, unless there is a public interest in over-ruling that request.
14. An e-mail folder for patient contacts will make it easier to delete these copies once the paper record has been filed.
15. Be aware that the patient may wish to – or may accidentally – forward your NHS e-mail to many other people. A factual message that complies with Section 4.3 of the E-mail policy – "Creating effective and appropriate e-mails" will maintain your professional standing.
16. Be aware that e-mail allows the patient to easily respond with information or attempt to begin an interminable back-and-forth correspondence.
17. Remember that the e-mail will form part of the printed patient record so it needs to clearly show the correct patient identifiers
18. Have an action plan if the email is returned as undelivered.
    - Check the e-mail address carefully. A comma instead of a full stop, or confusing 0 and O, can easily be corrected.
    - If e-mails are not read regularly, e-mails will be returned from a valid email address if the mailbox is full. Do not assume that the address is wrong.
    - If the e-mail is returned, have an alternative plan to contact the patient. And record in the notes what happened.
    - Be aware that the e-mail may be received successfully, but then not read, or accidentally deleted before it is read.
    - Be aware that the e-mail may be altered before the intended recipient receives it. Be ready to check that the patient saw your original document.
19. Always comply with the Trusts E-mail policy

IM&T POLICIES APPENDIX G

eMail & Internet Usage – Defamation & Libel

What is defamation & libel?
A published (spoken or written) statement or series or statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

What you must not do
Make statements about people or organisations on any web pages you are including on the website without verifying their basis in fact.

What are the consequences of not following this policy?
Individual Users and the Trust may be subject to expensive legal action.

Harassment

What is harassment?
Unwanted conduct that violates a person's dignity or creates an intimidating,
Hostile, degrading, humiliating or offensive environment for them having regard to all the circumstances including the perception of the victim
A key point to note in this definition is that:
It is the impact on the recipient or victim which is the determining factor in claims of harassment, and not the intention of the perpetrator.

What you must not do
Use the internet to harass other members of staff by displaying particular web sites that they consider offensive or threatening.

What are the consequences of not following this policy?
The Trust deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be made subject to the Trust's Disciplinary procedure. *Any proven case of harassment will result in disciplinary action against the guilty party which could ultimately lead to their dismissal.*

Pornography

What is pornography?
Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography that is legal in the UK may be considered illegal elsewhere. Because of the global nature of Internet these issues must be taken into consideration. Therefore, the Trust defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Trust will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

What you must not do

- Create, download or transmit (other than for properly authorised and lawful research) pornography.
- Send or forward webmail's with attachments containing pornography. If you receive a webmail with an attachment containing pornography you should report it to the ICT Help Desk or your supervisor.

What are the consequences of not following this policy?

- Users and/or the Trust can be prosecuted or held liable for transmitting or downloading pornographic material, in the UK and elsewhere.
- The reputation of the Trust will be seriously questioned if its systems have been used to access or transmit pornographic material and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, may be subject to disciplinary or even legal action.

Copyright

What is copyright?

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. The Organisation purchases licences on behalf of its users.

What you must not do

- Alter any software programs, graphics etc. without the express permission of the owner.
- Claim someone else's work is your own
- Send copyrighted material by Internet without the permission of the owner. This is considered copying.

What are the consequences of not following this policy?

A user and/or the Organisation can face fines and/or up to two years imprisonment for infringing copyright.

IM&T POLICIES APPENDIX H

Internet Usage – Guidance on using social media

SCAS recognises that social networking and photo sharing web sites such as Facebook, Twitter and SnapChat are now perceived as every day methods to keep in contact with friends, make public statements, upload photographs and to advertise / review events. Though the actual solutions change as frequently as public taste their impact and potential to reach a wide audience is constant.

The Trust urges staff to use any sites sensibly and responsibly and to consider the wider implications of using social networking sites outside of work.

Whilst you are entitled to a private life, it is up to you to ensure that you are not breaching the Trust's IT policies or reasonable conduct guidelines when using Facebook or similar sites whether at work or outside of work. As a guide, you should ensure, when posting, that you do not:

- Breach patient/staff/Trust confidentiality
- Post any material that has the potential to bring the Trust into disrepute – this may include

    - inappropriate comments and/or photos
    - malicious allegations against other Trust employees or the Trust itself which could constitute discrimination, bullying or harassment

Staff should recognise that it is inappropriate to be using Social Networking sites whilst working – cases recorded to date which have resulted in disciplinary action include staff messaging each other using mobile telephones whilst on duty, staff posting inappropriate comments to a site during meetings and staff found to be playing games online during working hours.

The above list is not exhaustive and failure to comply with the Trust's guidelines may constitute Misconduct or Gross Misconduct in accordance with the Trust's Disciplinary Policy. This is, of course, the case regardless of whether the misconduct occurs on-line or off-line but it is worth re-iterating that such misconduct on-line will be treated just as seriously as in other domains and may result in disciplinary action.

It is hoped that by following the guidelines above for reasonable use that staff will avoid placing themselves and / or the Trust in a compromising position through inappropriate posts on the Interne

IM&T POLICIES APPENDIX I

Examples of Types of Reportable ICT Events

These examples are indicative only and do not constitute an exhaustive list.

1) The disclosure of confidential information to any unauthorised individual.

- A member of the public viewing assessment records left on a reception desk.
- A member of staff accessing data on SCAS systems relating to family or friends.
- A member of staff "browsing" through assessment records in an open area.

2) Events affecting the integrity of a system or data being put at risk.

- Someone loading unauthorised software (games etc.) on to a SCAS PC.
- Data being altered by a member of staff for no legitimate reason.
- Something odd happening on a screen when in use.
- Computer files disappearing from PC's or unknown files appearing.
- Sharing passwords.
- Using a PC for non-SCAS related purposes.
- Someone connecting a non SCAS device to a network cable

3) Events affecting the availability of the system or information being put at risk.

- An unidentified or unaccompanied stranger seen carrying computer equipment or SCAS paper files

4) Events having an adverse impact, i.e. something which;

- Could cause embarrassment to SCAS or the NHS
- Threatens personal safety or privacy
- Breaches legal obligations
- Causes financial loss or disrupts activities

IM&T POLICIES APPENDIX X

Acronyms

DPA – **D**ata **P**rotection **A**ct 1998

ICT – **I**nformation and **C**ommunications **T**echnology

IM&T – **I**nformation **M**anagement & **T**echnology

IT – **I**nformation **T**echnology

NHS – **N**ational **H**ealth **S**ervice

SCAS – **S**outh **C**entral **A**mbulance **S**ervice NHS Foundation Trust

SIRO – **S**enior **I**nformation **R**isk **O**wner

VPN – **V**irtual **P**rivate **N**etwork

Wi-Fi – A wireless networking technology allowing devices to connect wirelessly