Essex Partnership University
NHS Foundation Trust

IT&T SECURITY PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG50a
VERSION NUMBER:	2.5
KEY CHANGES FROM PREVIOUS VERSION	Guidance on Mobile Phones (s7.19) added; 3 month extension (March 21 GC)
AUTHOR:	[redacted]
IMPLEMENTATION DATE:	November 2020
AMENDMENT DATE(S):	March 2018; May 2020; July 2020, October 2020
LAST REVIEW DATE:	March 2018
NEXT REVIEW DATE:	~~March~~ June 2021
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE	March 2018
RATIFICATION BY QUALITY COMMITTEE:	N/A
COPYRIGHT	

POLICY SUMMARY

These procedural guidelines will reduce the risk associated with not having a procedure document in relation to information governance / security and access to Trust facilities (IT, Email, Internet, Portable Media) is an uncoordinated approach to its safe use which could render the Trust vulnerable in terms of legal implications of staff use of facilities and lack of organisational controls to safeguard users and the Trust.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this procedure, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate.

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this procedure is Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

IT&T SECURITY PROCEDURE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – CLICK ON THE SECTION HEADINGS BELOW TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

IT&T SECURITY PROCEDURE

1.0 INTRODUCTION

1.1 These procedural guidelines aim to set out the South Essex Partnership University NHS Foundation Trust's (the "Trust") rules relating to information security and apply to all business functions and cover all information systems, networks, physical environment and relevant people who support those business functions.

1.2 Areas of information governance / security covered within the body of these procedural guidelines include:

- Security for Job Definitions & Resourcing
- Security Control of Assets
- Personal Security
- Physical / Environment Security
- Communications
- Access Control
- Systems Development
- Business Continuity

2.0 SECURITY FOR JOB DEFINITIONS AND RESOURCING

2.1 The objective of Security for Job Definitions and Resourcing is to reduce the risks of human error, theft, fraud or misuse of facilities. To ensure that users are aware of information security threats and concerns, and are equipped to support the Trust's security policy in the course of their normal working practices.

2.2 Job definitions

2.2.1 Security should be addressed at the recruitment stage and be included in staff job descriptions and contracts, and monitored during employment.

2.2.2 Managers should ensure that where staff are required to use IT&T they are briefed and encouraged to have sight of the Information Governance and Security Policy (CP50) and associated legislation including the Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR), Freedom of Information Act 2000, Copyright, Designs and Patents Act 1988 and Computer Misuse Act 1990 etc. Staff should also be made aware of conduct and disciplinary procedures, which may be invoked should a breach of security arise.

2.2.3 **All** staff are accountable for the functions they perform.

2.2.4 It is essential that significant work performed by any key staff can be taken over by someone else in the event of the unavailability of the key person.

2.2.5 Expertise should be shared. For critical systems, training should be given to at least two staff so that in the absence of one, work may continue in the critical area by the other.

2.2.6 Staff should be fully aware of the extent of their authority, particularly their individual tasks and budgetary responsibilities.

2.2.7 IT&T privileges and access rights should be allocated on the basis of the specific job function, and not on the status or standing of the job.

2.2.8 Personal interest should be declared in circumstances that could lead to a conflict of interest. This is of specific importance where IT&T procurements are involved.

2.2.9 Contractors should be notified of the IT&T security procedures and should sign an agreement to which they must abide. These are the same codes of conduct and discipline as permanent staff. Where contractors are employed through an agency the conditions should form part of the contract with the agency. If work of a sensitive nature is to be performed by contract personnel then extra conditions should be identified and imposed in accordance with this greater risk exposure.

2.2.10 Reference requests during recruitment should also indicate IT&T security matters.

2.3 Confidentiality Agreement

2.3.1 Users of IT&T equipment will sign a non-disclosure undertaking (confidentiality agreement). This understanding will form part of the contract of employment and the conditions in the undertaking should be clearly explained.

2.3.2 Where agency and contract staff and other third party users are not already covered by a non-disclosure undertaking in their existing contract they must sign a confidentiality agreement before they are connected to the Trust's IT&T facilities.

2.3.3 Confidentiality agreements should be the subject of review where there are changes to terms and conditions for employed staff or for contractors.

2.3.4 Where employees or contractors leave:

- The manager should confirm that the confidentiality agreement will continue to apply even though the person is leaving;
- Passwords and combination security doors should be changed to deny access, either by design or accident;
- Relevant departments should be informed of the changes;
- The name should be removed from all Trust directories, including email;
- All Trust property must be returned, particularly personal identification, entry keys, computer equipment and mobile devices;
- Emails cleared in the event of an NHSmail account (as address taken with the employee)

2.3.5 Particular attention should be paid to the above if the employment termination is not 'amicable'.

3.0 DEFINITIONS

3.1 ***IT&T*** – Information Technology & Telecommunications

3.2 ***The Trust*** – Essex Partnership University NHS foundation Trust (EPUT)

3.3 ***Network Assets*** – A collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by various means and created to share data, software, and peripherals such as printers, modems, fax machines, internet connections, CD-ROM and back-up tapes, hard disks and other data storage equipment.

3.4 ***Information Assets*** – (examples below)

Personal/Other Information	***Software***
Databases and data files, Back-up and archive data, Audit data, Paper records and reports,	Applications and System Software, Data encryption utilities, Development and Maintenance tools,
System/Process Documentation	***Hardware***
System information and Documentation, Operations and support procedures, Manuals and training materials, Contracts and agreements, Business continuity plans,	Computing hardware including PCs, Laptops, PDA, communications Devices e.g. blackberry and removable Media,
	Miscellaneous
	Environmental services e.g. power and air-conditioning, People skills and experience.

3.5 ***Removable Media*** – Includes back-up tapes, external & removable hard drives, DVD, CD-ROM and Memory Sticks (encrypted USB storage devices).

3.6 ***Confidential Sensitive / Person-Identifiable Information (PII)*** – Includes; person's name, address, full postcode, and date of birth; pictures, photos, videos, audio tapes or other images of patients/residents; NHS number and local identifier codes and anything that could be used to identify a patient or resident directly or indirectly e.g. rare diseases, drug treatments or statistical analyses which have very small numbers in a small population.

*** *Please note*** that the list above is not exhausted.

3.7 ***Faults*** – Examples below (All faults need to be reported to the IT Service Provider helpdesk via email/phone);
- Computer not switching on
- Encryption / Passwords need to be changed or reset
- Printer not working
- Network drives have disappeared

*** *Please note*** that the list above is not exhausted.

4.0 SECURITY CONTROL OF ASSETS

4.1 All major Trust assets should be accounted for and have a nominated owner for security purposes. Owners will have responsibility for maintaining appropriate security measures. Responsibility for implementing relevant security measures may be delegated, although accountability should remain with the nominated owner.

4.2 All equipment sited within a directorate or department in the South of the county will be the responsibility either of the director or head of that department. This generally means that the responsibility for security of PC's, including processor, monitor and printer will lie within the directorate where the equipment is held and used. For the North of the county all equipment is the responsibility of the North's ICT Services.

4.3 Information security classifications will be used to indicate the level and priority of security protection, including:

"Personal Data"
Means any information relation to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Special categories of personal data"(sensitive) Article 9
Means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Confidentiality (NHS Code of Practice)

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

- It is a legal obligation that is derived from case law.
- It is a requirement established within professional codes of conduct; and It must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures

5.0 PERSONNEL SECURITY

5.1 **Personnel security** must be addressed at the recruitment stage and should serve the purpose of:

- Providing direction to the Trust on personnel security and ensure that appropriate personnel security structures are in place regarding awareness training to new Trust employees concerning their information security responsibilities.
- Ensure that procedures are in place to reduce the risks of human error, theft, fraud or misuse of Trust facilities, and to ensure that all staff are aware of the requirement to maintain the confidentiality of information and the security of information processing facilities.

5.2 **Including Security in Job Responsibilities**

5.2.1 Every job description must outline the following points:

- An employee's responsibilities regarding information security.
- That employees are required to be aware of the Trust's policy on information security.
- That employees are responsible for security in relation to their job role.
- Employees should be familiar with other related trust policies, including Information Classification, Data Protection and Confidentiality Policy and security incident reporting procedures.

5.2.2 Contracts must clearly state that any breach of, or refusal to comply, with Trust policies is a disciplinary offence, which may lead to disciplinary action.

5.3 **Personnel Screening Management of staff access to sensitive information**

5.3.1 The Trust will ensure that verification checks are undertaken on all new employees, whether permanent, temporary or contractors, in line with current recruitment policies.

5.3.2 Where staff are employed by other organisations (e.g. agencies), the supplying organisation's contract must set out the responsibilities to

undertake relevant checks to a similar level on all staff who will work within the Trust.

5.3.3 The performance of all staff in respect of information security, especially those who have access to sensitive information, should be reviewed on a regular basis by line management.

5.4 Confidentiality Agreements

5.4.1 All employee contracts will include a confidentiality and non-disclosure clause, and must also include reference to the employee's legal responsibilities under the Data Protection Act 2018, General Data Protection Regulation and Computer Misuse Act 1990.

5.4.2 Individuals who are not employed or contracted to the Trust but who have access to, or may come into contact with, confidential information must sign an appropriate confidentiality agreement before access is permitted (e.g. work experience staff who may have access to confidential information).

5.5 Terms and Conditions of Employment

5.5.1 The employee's terms and conditions of employment will clearly state what their responsibilities are regarding security and confidentiality of information within the Trust.

5.6 Information Security Education and Training

5.6.1 The Trust will ensure that all employees are provided with appropriate training in information security as part of their induction process, and are provided with an additional mandatory training programme to update their information security awareness on an annual basis.

5.6.2 The Trust will also ensure that all employees are made aware of updates to the information security policies, and that these policies are readily available.

5.7 Responding to and Reporting Security Incidents, Weaknesses and Malfunctions

5.7.1 The Trust will ensure that all employees are made aware of the information security incident reporting procedures (CPG50(E)) and that they understand the requirement and process for reporting such incidents.

5.7.2 All Trust employees are responsible for reporting information security related incidents, weaknesses and malfunctions as soon as practicable after they are discovered.

5.7.3 All information security related incidents must be reported to the Trust's Information Governance Manager (Information Security Officer/s designate), or to the Director of ITT using the procedure identified in CPG9(F) (Records Management Policy – Information Security Incident Management Procedure).

5.8 Learning from Incidents

5.8.1 The Director of ITT must ensure that all reported information security incidents are recorded in the Information Security Register to ensure that monitoring costs and impacts of all incidents can be carried out across the Trust. All information security related incidents will be reported to and reviewed by the Information Governance Steering Sub-Committee.

5.9 Disciplinary Process

5.9.1 Any violation of these security procedural guidelines or related policies will be handled in accordance with the Trust's Disciplinary Policy and Procedures.

6.0 PHYSICAL / ENVIRONMENTAL SECURITY

6.1 Physical Security / Securing Offices, Rooms and Facilities

6.1.1 Access to data held on the Trust's information systems can be minimised by restricting physical access to Trust buildings.

6.1.2 Signage for buildings, offices and other areas should only give the minimum indication of purpose.

6.1.3 Where information is kept in offices, access to buildings must be restricted. These restrictions include making sure security doors are closed properly and entry codes are changed regularly (see also RM09 Management of Security Policy).

6.1.4 Within any area there should be the facility to protect information and information processing facilities. These facilities may be lockable offices or filing cabinets. As far as possible staff should use these facilities to safeguard and protect information.

6.1.5 Doors and windows should be locked when unattended, with external protection considered for windows, particularly at ground level.

6.1.6 Visitors to non-patient/non-resident areas in Trust buildings should be accompanied at all times and should sign in and out of premises on arrival and departure.

6.2 Equipment Security

6.2.1 In order to prevent loss, damage or compromise of assets and interruption to any Trust business activities all equipment should be physically protected from security threats and environmental hazards.

6.2.2 Protection of IT&T equipment is necessary to reduce the risk of unauthorised access to information and to safeguard against loss or damage.

6.3 Equipment Siting and Protection

6.3.1 For areas where corporate servers are stored the appropriate environment should be maintained (e.g. temperature, humidity and power supply quality).

6.3.2 Corrective action will be taken when any of the above is detected, normally on behalf of the Trust by IT&T staff, using maintenance support arrangements

6.3.3 The Trust operates a no smoking policy in all buildings and locations and eating and drinking are not allowed in designated computer rooms.

6.4 Power Supplies

6.4.1 It is the policy of the Trust to protect critical equipment (e.g. clinical and corporate systems) from power failure. A suitable supply, as dictated by manufactures' specification, will be available, with backup power supplies available when required.

6.5 Equipment Maintenance

6.5.1 Ongoing maintenance of computer equipment will normally be subject to a maintenance agreement. However, under certain circumstances it may be more cost effective to replace equipment rather than continue to maintain. Under these circumstances the Director of ITT will decide whether this course of action will be beneficial to the Trust.

6.5.2 System engineers allowed into Trust premises must identify themselves as belonging to the maintenance company, and must adhere to the general procedures adopted for all visitors.

6.5.3 Where an information medium (e.g. computer hard drive, tape) has failed, the rectification process must result in the failed item being left with the Trust for secure destruction.

6.6 Security of Equipment off Premises

6.6.1 Equipment taken off Trust premises should only be done with the approval of the appropriate manager or Head of ITT Service Delivery. Laptop computers will be protected by suitable access protection and drive encryption. Staff who have obtained authorisation to take equipment off of Trust premises should ensure that such equipment is given a high level of protection. Equipment must not be left in cars as the high incidence of car theft leads to a substantial level of risk for the Trust's equipment and information.

6.7 Secure Disposal of Equipment

6.7.1 All items of equipment that store data must be disposed using the Trust's ICT service provider.

6.8 General Controls – Clear Desk/Clear Screen Policy

6.8.1 Information left unattended on desks or displayed on computer screens is liable to unauthorised disclosure, modification or removal. The Trust operates a 'clear desk' and 'clear screen' policy, covering paper information, removable storage media and information displayed on computer screens. Where appropriate, paper and computer media containing sensitive information should be stored in suitable locked cabinets when not in use. Computers / telephones must not be left logged on when unattended.

6.8.2 Sensitive or confidential information, when printed, must be removed from printers, photocopiers and fax machines immediately. Incoming and outgoing mail points and fax machines must be protected from unauthorised access. Where information is transferred by fax, appropriate measures must be taken to ensure that there is no accidental disclosure. Reference should be made to Trust policy CPG9(E) Safe Haven Procedure.

7.0 COMMUNICATIONS & OPERATIONS MANAGEMENT

7.1 This section provides guidance in the following areas:

- The secure operation of information processing facilities
- The minimisation of risk of system failures
- The protection and maintenance of the integrity and availability of software, information and information processing and communication facilities.

In addition:

- To ensure that information within networks and their supporting services is adequately protected
- To ensure the Trust assets are protected and that interruption to business activities is minimised.
- To prevent loss, modification or misuse of information.

7.2 Operational Procedures and Responsibilities

7.2.1 The Trust must ensure that all operating procedures identified within the IT&T Security procedure are documented and maintained. Changes to these documents must be authorised by Director of ITT. Operating procedures must specify the detailed instructions for the implementation of each job, including:

- Processing and handling information, including confidentiality requirements and information classifications.
- Work scheduling requirements.
- Instructions for handling errors or other exceptional conditions, including restricting the use of system utilities.
- Contacts for support in the event of technical or operational difficulties.
- Any instruction for handling special stationery or other special system out- puts.

- Detailed system start and recovery procedures to be followed in the event of a system failure.
- Procedures for system housekeeping, backups, equipment maintenance, and computer room usage.

7.2.2 Changes to information processing facilities and systems must be controlled. The Trust must have in place formal documentation change control mechanisms, including:

- Identification and recording of significant changes and assessment of their potential impact.
- Formal approval for proposed changes.
- Communication of changes to all relevant personnel.
- Procedures for aborting and recovering from planned unsuccessful changes.

7.2.3 The Trust must have in place documented Incident Management Procedures to ensure an effective response to information security incidents.

7.2.4 The Trust should, where appropriate, ensure that segregation of duties is in place on all systems, in order to reduce the opportunities for unauthorised modification, or misuse of information and information systems. The Trust must also ensure that, where possible, development, test and operational facilities are segregated. Where possible, development and operational systems should be run on different processors, or in different domains or directories.

7.2.5 Where an external contractor is used to manage processing facilities, the Trust must ensure that an appropriate risk assessment has been undertaken and that appropriate controls have been agreed to reduce any potential exposure to damage or loss of information. These controls must be incorporated into any contracts that are established.

7.3 System Planning and Acceptance

7.3.1 The Trust must ensure demands on system capacity are monitored and projections of future capacity requirements are made to ensure that it has adequate processing and storage facilities available. The utilisation of key system resources, such as file servers, e-mail servers and business critical systems should be monitored so that additional capacity can be brought online when required.

7.3.2 The Trust must have in place acceptance criteria for new information systems, for upgrades and new versions. All such changes must be tested prior to acceptance.

7.3.3 Specific responsibility for planning network facilities and change control of the network rests with the Director of ITT. The IT&T Department shall maintain a comprehensive plan of the network, documenting all major components and cable structures.

7.3.4 Any new cabling installations shall be planned to reduce the risk of unauthorised physical tampering or connection. All cabling running 'public access' areas should be hidden in roof spaces or ducting to minimise the risk from malicious damage.

7.3.5 A standard, documented directory structure shall be implemented across all network file servers. All users shall be provided with a directory for the storage of business files. All other directory allocations shall be documented and based upon specific business needs.

7.4 Protection against Malicious Software

7.4.1 The Trust must have in place formal controls to detect and prevent malicious software from entering the network. These controls must, as a minimum, include:

- Compliance with software licensing.
- Compliance covering obtaining and introduction of files and software either from or via external networks.
- Installation and regular update of anti-virus detection and repair software.
- Procedures for dealing with viruses and business continuity plans for recovering from virus attacks.

7.5 Housekeeping

7.5.1 In order to allow the Trust to recover as quickly as possible in the event of data loss or corruption on one or more of its computers systems data essential to the business of the Trust must be backed-up. In order to achieve this there must be set procedures to cover:

- The copying of data to a medium, which can then be stored in a secure location (back-up).
- The retrieval of data from copy made on the selected medium (restore).
- The secure storage of media containing the data containing the data copies.
- The recording of details about the media and what data is stored in order to facilitate the easy and correct identification of a particular item of storage media when it is necessary to retrieve data from it.
- Testing the quality of the back-ups made both by log checking, verification and by test retrieval of data from an item of storage media.

7.5.2 The Trust must ensure that all faults reported by users regarding problems with information processing or communications systems are logged, along with the corrective action taken.

7.6 Network Management

7.6.1 The Trust must ensure that appropriate mechanisms are in place to all protect Trust Networks from unauthorised access and to protect the security of data within the network and connected services. Where possible the following should be adopted, including:

- Operational responsibility for the network should be separated from computer operations, where appropriate.
- Responsibilities for the management of remote equipment and remote access to the network must be identified.
- Where appropriate, special controls should be implemented to protect the integrity of information passing over public networks, such as the use of encryption and digital signatures.
- The network architecture should be specially documented, including the planned detailed settings of all hardware and software components.

7.7 Media Handling and Security

7.7.1 The Trust must put in place procedures for the appropriate handling and security of removable computer media such as tapes, disks, memory sticks / flash drives (USB devices), cassettes and printed media (reports). Procedures should include, the requirement to erase the previous contents of any re-usable media when no longer required, formal authorisation for the removal of media from the Trust and the requirement for media to be stored in a secure manner.

7.7.2 The ICT Service provider is responsible for the secure destruction of all data media that is no longer required.

7.7.3 The handling and storage of information must be conducted in line with the GDPR & Data Protection Act 2018.

7.8 Information and Software Exchange

7.8.1 In order to prevent loss, modification or misuse of information the Trust should ensure that the exchange of information and software between organisations should be controlled by the adherence to the N3 National Network, and any agreed Data Sharing Protocols.

7.8.2 The exchange of information and software between organisations should be controlled. For physical transport, reliable couriers should be used at all times. Where necessary, special measures should be adopted to protect sensitive information from unauthorised disclosure.

7.9 Security of Electronic mail

7.9.1 When using the electronic mail system, staff must be particularly aware of the following:

- Vulnerability to unauthorised interception or modification;
- Vulnerability to incorrect addressing;
- Vulnerability to possible virus attachments.

7.9.2 Consideration should also be given to:

- The requirement to exclude sensitive information from the system;
- The exclusion of third parties from e-mail services.

- The use of NHS approved encryption techniques as they become available (i.e. NHSmail (@nhs.net) for the secure transfer of person identifiable information via email).

7.10 **Permitted use**

7.10.1 Trust staff should use email for business purposes, including sending patient/ resident data (following assessment of risk and application of controls, such as password protecting documents).

7.10.2 IT&T services uses software to monitor the use of emails and can intercept inappropriate attachments, which will be reported to the Trust's Data Protection Officer/s as a breach of the GDPR & Data Protection Act 2018.

7.10.3 The Trust authorises Limited 'personal use' of its email facilities.

7.11 **Non-permitted use**

7.11.1 Staff must not use the Trust's email facilities for excessive personal use, or private gain. Sending offensive, defamatory material or breach confidentiality is also forbidden. Any such breaches may be subject to the Trust's disciplinary procedures.

7.12 **Security of Electronic Office Systems**

7.12.1 The Trust's electronic information resources are vital assets, which require appropriate safeguards. Electronic office systems are vulnerable to a variety of threats, which may compromise the confidentiality, integrity and availability of information.

7.12.2 Electronic office systems includes Calendar, systems such as Outlook, Word processing, spreadsheets, databases and underlying electronic infrastructure required to operate such systems. The following controls should therefore be applied:

- All users, along with line managers, are responsible for controlling access to their calendars. Any delegated access should be provided strictly on a 'need-to-know' basis.
- The Trust will provide the infrastructure to allow staff to save files and documents to shared network drives that are regularly backed up.
- Line managers will be responsible for authorising which staff are allowed to access appropriate areas of shared network drives and folders.
- Users are responsible for deleting files when no longer required.

7.13 **Publicly available systems**

7.13.1 Access for Trust staff to certain websites on the internet will be controlled by a request and authorisation process, and monitored by IT&T.

7.14 Information transmitted via telephone, fax and post

The following minimum standards will be applied:

7.14.1 Telephone conversations (including answer-phones):

- No personal information shall be given out over the telephone without best endeavours by the member of staff to confirm the identity of the other party, and the wishes of the individual concerned.
- Telephone calls that may feature personal or sensitive information about any individual will be made in private areas if at all possible.
- If an answer-phone message is left, minimal information will be provided.

7.14.2 Fax:

Reference should be made to the Trust's Safe Haven Procedure CPG9(E). However, the following points should be adhered to, including:

- Faxes must be sent to named individuals.
- All Faxes must be preceded by a cover sheet.
- Fax machines must be sited away from public areas.
- Minimal information will be transmitted.
- The intended recipient must be notified prior to sending.
- The Trust must designate specific fax machine locations as a 'safe haven', where patient/resident and sensitive information can be transmitted and received in a secure environment.

7.14.3 Post:

- All post should be sent to a named individual, where possible.
- All post will be marked 'Private and confidential' if it contains personal and/or sensitive information and will not be sent in re-seal envelopes.
- A P.O Box return address should be on the reverse of the envelope.
- Window envelopes should be used – a handwritten address is not advised.

7.15 Information Transmitted via email and Internet

7.15.1 All staff should be aware of the procedures relating to email and internet use and should read the Email / Internet Access and Use Procedure (CPG50(B)) for further information.

7.16 Video Consultations / Video Conferencing (VC)

7.16.1 Video conferencing is a live audio and video conversation between 2 or more people in different locations, conducted using phone, tablet, laptop or desktop computer.

7.16.2 The Trust has approved the use of the following applications:

- Microsoft Teams
- accuRx
- Attend Anywhere

7.16.3 Key considerations regarding the use of VC applications are below:

Users of are reminded of their obligation to complete the mandatory Information Governance e-learning module on an annual basis.

- VC should be used for business purposes in line with Trust Information & Security policies / Record Management policies / professional codes of practice / Data Protection Act 2018 / General Data Protection Regulation 2016.
- Users are reminded that ALL information created within Teams is saved to a library, which is a **temporary** SharePoint site. Teams is designed as a tool to help collaboration, not as a permanent way to store records. Users **MUST** adhere to their professional codes of practice, the policies listed above and contractual requirements to information and records are appropriately managed. Do not use Teams as a permanent records store.
- Teams is not a clinical or workforce system. The disclosure and storage of personal and confidential information should be kept to a minimum and appropriate security measures applied.
- Regularly review Team membership and take account of movers and leavers.
- Consider the information shared during group calls/meetings, especially where participants are external to EPUT. Be aware that participants in group calls may be able to download any shared content and consider whether it is appropriate to share your screen.
- When offering a video consultation, ensure that the method you use to send the invitation is appropriate for the attendee to have, i.e. email address or mobile number. If it is not appropriate for the attendee to know your email address or mobile number, use a generic email account with a disclaimer (out of office response and/or signature) stating that email replies are not monitored.
- Information posted in the chat function of MS teams can be retained by any participant, ensure that any messages or content posted in the chat is appropriate to be shared with all attendees.

You must:

- notify your manager immediately if you receive any inappropriate material.
- comply with copyright law and all applicable licenses, which may apply to software, files, graphics, documents, messages and other material you wish to upload / to download or copy.

You must not:

- access, store or provide links to inappropriate non-business-related websites or other resources which display, store, make available or send material which is illegal, discriminatory, harassing, obscene, pornographic, libelous, defamatory, breaches any obligations of confidentiality or is otherwise deemed by EPUT to be inappropriate in the work place.
- Illegally copy material protected under copyright law or make material available to others for copying.

7.16.3 Recording within MS Teams

Recording meetings can be a useful way of capturing training sessions, allowing colleagues who could not join a meeting to catch up later, or as a reference for note taking afterwards. However, there are a few things that users should be aware of to ensure that the recording is secure, but accessible to the right people.

7.16.4 Five key things to know about recording meetings

1. When you record a Teams meeting it is stored temporarily (for 20 days) in the meeting chat history. Whoever initiates the recording is responsible for it throughout its lifecycle.
2. The recording is available to download by NHS.net staff participants only. Guests are not able to download.
3. Recordings are NOT uploaded to Microsoft Stream and can only be accessed once they are downloaded and saved on a secure network drive".
4. All recordings are subject to professional conduct and Information Governance standards. Please be mindful of what you discuss, record and share.
5. Recordings not downloaded will automatically expire and delete after 20 days and will not be available for download.

7.16.5 Whoever initiates a recording is the owner of that recording, and it is their responsibility to ensure that:

- Everyone being recorded is aware of and in agreement with the meeting being recorded.
- If the recording is downloaded, it is held securely and deleted as soon as it has been used for its specific purpose – for example, if used as a reference to take minutes, the recording should be deleted as soon as the minutes have been approved.

7.16.6 Governance of recordings

Be aware that anything you record could be made available under:

- Freedom of Information (Scotland) Act
- Subject Access Requests, under the General Data Protection Regulations
- Data Protection Act (2018)
- Other authorised and agreed international standards and regulations.

Therefore, be mindful of what is discussed, recorded and shared. If in doubt ask EPUT's Data Protection Officer, Information Governance representative and records managers for advice about data protection and information management.

7.17 **USB 'Memory Sticks'**

7.17.1 A USB device, 'memory sticks', is a mobile storage device, which holds a vast amount of data and can be easily plugged into a notebook or PC USB ports. It is convenient and easy to use, and the user can define a password for confidential data areas. Other names for USB 'memory sticks' include flash drive, pen drive and thumb drive.

7.17.2 **Only encrypted USB 'memory sticks' provided or sanctioned by the Trust** may be connected to any device on the Trust network.

7.17.3 Only IT&T Services will be permitted to purchase USB 'memory sticks', and a Register will be maintained for monitoring purposes.

7.17.4 The USB 'memory stick' must only be used for legitimate work purposes.

7.17.5 Any data held on USB 'memory sticks' must be password protected to protect contents from unauthorised access.

7.17.6 It will be the responsibility of the user to use due diligence to keep memory sticks secure at all times.

7.17.7 No patient or resident identifiable information is to be held on USB 'memory sticks'. They should only be used for transferring the data, then the data should be deleted. This applies only to Trust encrypted USB sticks.

7.17.8 Any loss of USB 'memory sticks' must be reported to the Trust's Data Protection Officer/s or Head of ITT Service Delivery immediately.

7.18 Other 'Plug-in' Devices

7.18.1 These devices include, but are not limited to:

- MP3 Players (which can hold more information than USB 'memory sticks')
- Smart Phones (mobile phones, which allow connection to PC's and run
- Various operating systems such as Windows CE
- Digital Cameras
- Compact Flash Cards
- External USB hard drives
- Firewall devices

7.18.2 These 'plug-in' devices are governed by the same 'acceptable use' criteria as with the above-mentioned USB 'memory sticks'

7.19 Mobile Phones

7.19.1 Only ITT Services will be permitted to purchase mobile phones and a register will be maintained for monitoring purposes. All mobile phones will be issued encrypted and with password protection and staff are responsible for ensuring they update passwords to a personal setting and then maintain the security of their passwords. It will be the responsibility of the user to use due diligence to keep mobile phones secure at all times.

7.19.2 Only mobile phones provided or sanctioned by the Trust may be connected to the Trust WiFi.

7.19.3 Mobile phones must be returned to ITT services when their intended use by the recipient is no longer needed.

7.19.4 The use of mobile phones for personal use is permitted at cost, however, no support is offered and any data loss resulting from work usage or incident resolution is not the responsibility of the Trust. If the device becomes non-functional through personal usage, the default response will be to perform a factory reset.

7.19.5 Mobile phones will be monitored for activity and usage relating to voice and data. Any excessive use will be investigated and could result in disciplinary action being taken against the member of staff.

7.19.6 If a mobile sim is present in a device, this must at no point be changed or tampered with.

7.19.7 Users should create, maintain and manage an iTunes account for use with the device. Any issues experienced with your account cannot be resolved by ITT services and you will be required to liaise directly with Apple on any such issues.

7.19.8 Dictation can be enabled for users on mobile phones on request via ITT services. It is the user's responsibility to ensure that any configuration

changes are followed and maintained to ensure no data is sent to third parties.

7.20 **Laptops or Tablets**

7.20.1 Only laptops provided or sanctioned by the Trust may be connected to any device on the Trust network and these must be used for legitimate work purposes.

7.20.2 Only IT&T Services will be permitted to purchase laptops or tablets and a register will be maintained for monitoring purposes. All laptops or tablets will be issued encrypted and with password protection and staff are responsible for ensuring they update passwords to a personal setting and then maintain the security of their passwords. It will be the responsibility of the user to use due diligence to keep laptops or tablets secure at all times.

7.20.3 No corporately sensitive / patient / resident / staff or other person identifiable information is to be held on laptops or tablets. When using laptops or tablets to work with person identifiable information this can only be done if the staff member has access to the Trust network via VPN (Virtual Private Network) or Work Smart set-ups.

7.20.4 No data should be held on the laptop or tablet's hard drive (C :\) at any time. If using a Trust laptop or tablet device for non-person identifiable data you should not save this to the hard drive but securely e-mail work on to a Trust network as soon as possible. Where a laptop or tablet is connected to the Trust's network information should be saved direct to the network drives.

7.21 **Reporting Incidents**

7.21.1 In the event of failure of any PC (desktop) or portable media device encryption, password or virus protection staff should immediately contact the IT&T service desk for advice and guidance as to continued use or repair requirements.

8.0 ACCESS CONTROL

8.1 Access to information should be controlled on the basis of business and security requirements and the user's role in the operation of the Trust.

8.2 Trust systems need to be strictly controlled to ensure that only those authorised can gain access and that access is defined on the basis of need. Access control is a requirement of current UK legislation.

8.2.1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate that processing is performed in accordance with this Regulation**. Those measures shall be reviewed and updated where

necessary.

8.2.2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

8.3 **System access control**

8.3.1 The following rules will be applied to controlling access to any information system within the Trust by any employee and third parties.

8.3.2 Access to systems and information will be on a 'need-to-know' basis.

8.3.3 Setup and regular maintenance of access controls in systems will take account of all relevant legislation and regulations. Advice should be sought from IT&T, who will in turn seek more specialist advice if required.

8.3.4 Access controls will be based on user roles, clinical speciality and geographical location.

8.3.5 All access controls will be reviewed regularly by IT&T.

8.3.6 As a general rule, certain administration staff should see little or no clinical information, accepting there are some administrative roles that will require access to such clinical information.

8.4 **User access management**

8.4.1 To prevent unauthorised access to information systems, formal procedures are in place to register access to Trust systems. These include:

- The formal completion of an access application form, which is endorsed by the users' immediate line manager and countersigned by the authorised signatory within IT&T.
- The use of unique user ID's to ensure that users can be linked to, and made responsible for, their actions.
- Maintenance of a formal record of all users.
- Immediate removal of access rights of users who have left the Trust, or changed operational role.

8.4.2 The Trust also ensures that the allocation and use of special privileges (i.e. administrator rights - the ability to override system or application controls) is restricted and controlled.

8.4.3 Access to all critical systems within the Trust is controlled by passwords, and the allocation is controlled through a formal management process.

8.4.4 Regular reviews to user access rights are carried out annually.

8.4.5 The Trust's Human Resource Department should ensure that all leavers are notified to IT&T in order prompt removal of redundant user accounts is carried out.

8.5 User Password Management

8.5.1 Most systems within the Trust require a log in name and password for access. All staff are given access rights and privileges to the various systems in accordance with the type of data they require to use. All staff will have a log-in for one or more of the network servers in addition to any other systems they use.

8.5.2 In all cases any passwords given to staff personally are for that individual only. Passwords should not be written down or given to others to use under any circumstances.

8.5.3 Passwords should be a minimum of 6 characters (see Appendix 1 – Setting Passwords Guidance) and should be a combination of letters and numbers and should be changed every 30 days as prompted on-screen.

8.5.4 Do not use familiar names, such as pet names, and if at all possible try not to use proper words. This makes the accidental discovery of a password more difficult.

8.5.5 Passwords must be kept confidential, and changed if users believe they have been compromised.

8.5.6 Some systems will prompt you when a password change is required, other do not. If they do not it is an individual's responsibility to change them.

8.5.7 If you suspect someone else may have detected your password, or you suspect someone else is using it you must change your password immediately and advise your manager.

8.6 Computer Security

8.6.1 All staff are responsible for all data they enter onto Trust computers. The very nature of the type of sensitive information staff deal with makes protection of that information of paramount importance.

8.6.2 All staff have a legal responsibility under the GDPR & DPA18 and the Computer Misuse Act to ensure that unauthorised access to data is prohibited and also that data is accurate and kept up-to-date. Such restrictions apply not only to people outside the Trust but may also apply to those in the Trust whose work does not necessitate access to the data. All staff must abide by the rules of the GDPR, Data Protection Act and Computer Misuse Act.

8.6.3 Never leave your computer unattended when it is logged on. Ensure that the lock facility on your computer is in operation.

8.6.4 Always ensure when leaving your place of work to log off and close down your computer correctly.

8.7 Network and Operating System Access Control

8.7.1 Access to Trust networks are restricted to authorised users only via a secure log-on process designed to minimise the opportunity for unauthorised access.

8.7.2 User access is restricted to those functions and applications that are required for the performance their duties.

8.7.3 The IT&T team is responsible for the issue of Network log-in accounts and also for email accounts, and the Service Desk is directly responsible for allocating access rights to staff wishing to access their systems.

8.7.4 Unsuccessful log-on attempts are restricted to three, whereby further attempts are blocked and the user must contact IT&T for verification and resetting of password rights.

8.8 Remote Access

8.8.1 Remote access is the ability to get access to a computer or network from a remote distance (i.e. home address).

8.8.2 For staff who require access to their email account the Trust will authorise connection via Outlook Web Access (OWA), which is a client/server remote access software solution based on Microsoft's .NET Framework.

8.8.3 For staff requiring access to the Trust network, including web resources, bespoke programs and network data, connection will be available through the Virtual Private Network (VPN) remote access facility. Reference should be made to Corporate Policy (CP30), Virtual Private Network (VPN) Remote Access to the Trust Data Network.

8.8.4 Staff wishing to utilise these facilities should contact the Head of ITT Service Delivery.

8.9 Network Shared Drives

8.9.1 It is the policy of the Trust to keep all data in a secure manner and to only allow authorised access to files to those who require the data as part of their normal duties. Unless there are specific reasons not to do so, all data files should be saved on the network file servers rather than on local PCs.

8.10 Viruses

8.10.1 It is the responsibility of all staff to protect the Trust's computer systems from viruses. All files received on any medium from outside the Trust (including those used on home computers) and any received via electronic mail must be checked for viruses before being used.

8.10.2 The Trust systems use sophisticated software to detect viruses. However, if you receive any emails that you are unsure of, or do not recognise the sender, do not open them. If you are unsure inform your manager.

8.11 **Backups**

8.11.1 The IT&T team will ensure all Trust servers and the files contained within are backed up on a daily basis.

8.11.2 It is the responsibility of individual users to back up any systems, which do not hold their data centrally.

8.11.3 All backups must be kept up-to-date and must be checked on a regular basis to ensure that it is possible to recover the data on them.

8.12 **Mobile Computing**

8.12.1 The Trust will ensure that mobile computing facilities are adequately protected to ensure that business information is not compromised. All staff whom use mobile computing facilities will receive adequate training and be aware of the increased security risks associated with storing information on these devices.

9.0 SYSTEM DEVELOPMENT & MAINTENANCE

9.1 To ensure that information governance controls are built into information systems and information processes, governance requirements will be built into systems from the outset. Suitable controls will ensure that management of purchasing new systems, together with the enhancement of existing systems, will ensure that information security is not compromised.

9.2 **Security Requirements of Systems**

9.2.1 The information governance lead will be involved in the development of new and existing information systems in order to provide advice on the appropriate security requirements, together with best practice for implementation.

9.2.2 IT&T system managers will be responsible for ensuring that appropriate security arrangements have been included in system specifications for new systems and system upgrades, and that all modifications to systems are logged and up-to-date documentation exists.

9.2.3 The Information governance, Data Protection Officer and Caldicott leads will ensure that full compliance with the GDPR, Data Protection Act 2018, common law duty of confidentiality and Caldicott requirements are paramount concerns of system and process developments.

9.3 **Security in Application Systems**

9.3.1 Application systems, wherever possible, will provide validation of all input to ensure that it is correct and appropriate. The following controls should be considered:

- Out-of-range values and invalid characters.
- Missing or incomplete data.

- Periodic review of the content of mandatory fields, or data files, to confirm their validity and inspection of hard copy input documents for any unauthorised changes.
- Defining responsibilities of staff involved in input processes.

9.3.2 Validation checks will be incorporated into systems in order to detect corruption of data that has been correctly inputted.

9.3.3 The new NHS Number should be used as the common identifier on all patient / resident records and correspondence. Local identifiers (e.g. hospital numbers) may be used.

9.3.4 The responsibility for review and development of input / collection validation will lie with the Director of ITT

9.3.5 Line managers of staff will have default responsibility to ensure their staff are aware of processes and procedures relating to the quality of inputted data.

9.3.6 Until such times as no further required, the Trust's Clinical Governance Audit Team will conduct a routine audit of paper-based records.

9.4 Security of System Files

9.4.1 All modifications to systems, including changes, updates and servicing of hardware, as well as software, must be conducted with security of paramount importance.

9.4.2 All software must be quality tested before general use. Where possible IT&T should test the reliability of any new or updated systems by running them in parallel with the old prior to installation.

9.4.3 Supplier software, which is used in systems, must be maintained at a level supported by the supplier, and any decision to upgrade must take into account the security of the release. Physical access should only be provided to suppliers for support purposes when necessary and must be with IT&T senior management approval. All supplier activity on systems must be monitored

9.5 Security in Development and Support Processes

9.5.1 Changes to any system must be assessed under a formal change control system. This must include an assessment of any changes and the impact on existing security. A record of all changes made must be logged, and must include:

- The identity of the person making the change
- Details of the changes made
- Any other systems affected by the changes
- Date and time of the change, with test results

9.5.2 When changes to operating systems are performed, application security should be reviewed to ensure that there is no adverse impact on existing security.

9.5.3 Access to data should wherever practical be limited to anonymised data and must be authorised by the data owner. Copies of data must be retained at the same levels of security and access controls as the original data. No testing must take place on 'live' data, including training or demonstration purposes.

10.0 BUSINESS CONTINUITY PLANNING

10.1 Business Continuity planning ensures that the Trust's essential business activities will be maintained in the event of any unforeseen major failure or disaster.

10.2 **Business Continuity Management**

10.2.1 The Trust is increasingly reliant on IT&T services in support of patient/ resident care. Any emergency affecting business critical systems may have a significant impact on the Trust's ability to continue its operations. Procedures must be developed, based on a Risk Assessment to recover affected systems and processes in order to ensure continuing operations within the Trust.

10.3 **Business Continuity Process**

10.3.1 The Trust will ensure that a managed process is in place for the maintenance of business continuity. The process must include:

- Understanding and identifying the risks to the Trust, this could result in the loss of vital systems or processes in terms of their likelihood and impact.
- Identifying and understanding the impacts, which interruptions are likely to have on the formulating and documenting business continuity plans for each of the Trust's business critical systems and processes.
- Regular testing and review of the plans and processes put in place.
- Ensuring that the business continuity plans are communicated throughout the Trust and that all affected staff are aware of what actions to take in the event of an emergency.
- Ensure that responsibility for the co-ordination of business continuity management is assigned at the appropriate level within the Trust.

10.4 **Business Continuity Planning Framework**

10.4.1 It is essential that there is a realistic continuity plan for each operational computer system, which identifies its essential elements and details the action to be taken to maintain these in the event of software or equipment failure. In the case of critical/corporate operational systems, continuity plans must be based on the availability of back-up computing facilities.

The continuity planning process must include:

- A formal documented assessment of how long users could manage without each computer system.
- A formal documented assessment of the criticality of each system, including the impact on the short, medium and long term loss of the system on business activities.
- Identification and agreement of all responsibilities and emergency arrangements.
- Documentation of agreed procedures and processes.

10.4.2 The Head of ITT Service Delivery will ensure that appropriate continuity plans are drawn up for all relevant systems.

10.4.3 The regular review of systems must also include the checking of continuity plans and that all staff receives relevant training, that documentation is up-to- date and that continuity plans are always is a 'state of readiness'.

10.5 **Testing and updating Business Continuity Plans**

10.5.1 The Trust must ensure that a testing schedule is in place, which sets out which elements of the plan are to be tested, when they are to be tested and who has responsibility for ensuring that the testing takes place. All tests should be monitored and documented.

10.5.2 Business Continuity Plans must be updated in the following circumstances, including:

- Changes to key personnel.
- Changes to contact details of personnel or system suppliers.
- Changes to location, facilities and resources
- Changes in legislation
- Changes to suppliers
- Changes to system or processes and identification of any new risks.

END