South Eastern Health and Social Care Trust

Policy Code: SET/Gen (115) 2015

Title:	**ICT - Security Policy**			
Author(s)	**Assistant Director of Technology & Telecommunications**			
Ownership:	**South Eastern Trust**			
Approval by:	**Ratified Directors as per signatory list**		**Approval date:**	**March 2015**
Operational Date:	**April 2018**		**Next Review:**	**March 2023**
Version No.	**3.2**	**Supersedes**	**SET/Gen (115) 2015 V3.1**	
Links to other policies	**ICT Master Policy** **ICT - Email Policy** **ICT - Internet Policy** **Setrust Email Encryption Guide**			

1.0 INTRODUCTION / PURPOSE OF POLICY

1.1 Background

With the increased number of computerised systems within the South Eastern Health and Social Care Trust (hereafter referred to as the Trust) and the wider HSC family the need for an appropriate ICT Security Policy to protect both patient/clients and staff is essential.

The transfer of personally identifiable / confidential information within the HSC provides major benefits for patients/clients, and for those involved in their care and treatment. However balanced with this is the need to protect the confidentiality of patient/client information.

Key legislative influences in the development of this policy include:

- The DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information (2012) - provides support and guidance, for all those involved in health and social care, concerning decisions about the protection, use and disclosure of service user information. .

- The General Data Protection Regulation(2018) GDPR provides the key statutory framework underpinning confidentiality in the health and social care sectors.

- The Freedom of Information Act (2000) deals with public access to official information. The Act gives the public a general right of access to information held by the Trust. The Act also requires the Trust to have an approved publication scheme, which is a means of providing access to information that the Trust publishes.

- The Investigatory Powers Act (2016) regulates the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications. It was introduced to take account of technological change such as the growth of the Internet and strong encryption.

- The Human Rights Act (1998) incorporates the Articles of the European Convention on Human Rights into domestic law. The Human Rights Act obliges all public authorities to protect people's Convention rights and requires all other legislation to be applied, if possible, in a way which protects those rights. Article 8(1) of the European Convention states that: 'Everyone has the right to respect for his private and family life, his home and his correspondence.' This Act may have significance in regard to this policy in the context of staff using Trust ICT equipment.

- The Computer Misuse Act (1990) makes illegal certain activities, such as hacking into other people's systems, misusing software, or helping a person to gain access to protected files of someone else's computer without his/her knowledge or approval.

- The Information Commissioner provides guidance and best practice for public authorities in respect to the aforementioned legislative Acts.

The information stored by the Trust on computer systems represents one of its most valuable assets. This information is at risk from many threats and there is a need to implement measures which preserve its confidentiality, integrity and availability. This policy provides detailed guidance on measures required to mitigate against ICT security risks and identifies roles and responsibilities of the Technology & Telecoms Department, Line Managers and staff users.

1.2 Purpose Of Policy

This policy provides a summary of the required principles, values, structures and roles and responsibilities of all staff in relation to ICT security.

This policy should be read in conjunction with other related Trust Policies.

This policy provides clarity in relation to where and to whom the policy applies and also includes situations where the policy does not apply.

2.0 DEFINITIONS/SCOPE OF THE POLICY

This policy applies to all users of SET ICT equipment and services.

3.0 ROLES/RESPONSIBILITIES

3.1 Chief Executive

The Trust Chief Executive is responsible for:

1. ICT security to the Chief Executive of the Health and Social Care Board

2. Nominating an ICT Security Officer (ITSO) to have responsibility for implementing, monitoring and promoting 'ICT Security Policy'. This is the Assistant Director of Technology & Telecoms.

3. Ensuring that the Trust ICT Security policy is consistent with HSC IS standards and policies.

4. Ensuring that all Information Systems (IS) in use are appropriately assessed for security compliance and are protected in accordance with the Security Policy.

5. Ensuring that the HSC ICT security standards are implemented effectively and regularly reviewed.

3.2 ICT Security Officer

1. The Trust nominated officer with responsibility for co-ordinating ICT Security is the Assistant Director of Technology & Telecoms.

2. This role will provide a Trust focus for all ICT security issues including an ICT security programme to implement, monitor and maintain the ICT security policy. The Assistant Director of Technology & Telecoms delegates the key activities of this role to the designated ICT Technical Officer within the ICT Department.

3.3 ICT Technical Officer

The designated ICT Technical Officer is responsible for:

1. Providing a focus for all ICT security issues in the Trust.

2. Receive and consider reports of ICT security incidents, initiating appropriate action and passing the reports to the HSC ICT Security Officer within the Business Services Organisation (BSO) as appropriate.

3. Establish, implement, monitor and promote ICT Security procedures.

4. Monitor the effectiveness of ICT security and initiate change where required.

5. Support the risk assessment of systems.

6. Co-ordinate and provide advice to System Managers on ICT security issues.

7. Assist in the development and maintenance of appropriate ICT contingency / continuity plans.

8. Liaise with regional ICT Security Forum and appropriate groups.

3.4 System Managers / Administrators

System Managers are responsible for:

1. All data held on their particular system and ensuring that it complies with Data Protection legislation.

2. Managing ICT Security measures including regular reviews of effectiveness and reporting all incidents to ITSO and taking action as appropriate

3. Unauthorised system access or attempted access to be reported on IR1 form and appropriate action taken. Information relating to ICT security must only be released by authorised process

4. In conjunction with ITSO to ensure that a contingency / continuity plan is maintained for the system. providingf assurance that regular backups are taken, documented and recoverable
   A formal process to manage users' access rights including active management of user accounts

   The process must ensure that access rights are reviewed regularly and that authorisation for special privileged access rights must be reviewed more frequently.

   Generic/group accounts require Information Asset Owner IAO's authorisation.

   NB privileges should be configured on the basis of least privilege

5. Implementation of an appropriate level of Password Control where available

6. Ensure all authorised users are aware of security policy and procedures.

7.

8. System auditing and monitoring

   - To ensure that licensing compliance is maintained (ICT can provide information support)

   - Audit checks must be limited to read-only access to software and data. All access must be monitored and logged.
   - Where possible system log files to record successful/failed log in attempts.

9. Ensure relevant Data Access Agreements are in place and reviewed regularly.

3.5 Staff / Users

1. Staff / Users are responsible for:

   a. Complying with the Trust 'ICT Security Policy' and all extant legislation.
   b. Update MyDetails regularly ensuring location, contact numbers and line manager are accurate
   c. Line Managers should ensure staff have update MyDetails as appropriate.

d. Complying with all Information Governance Policies.
e. Notifying the System Manager of ICT Security Breaches which come to their attention.
f. Ensuring that their corporate portable ICT Equipment has encryption software if sensitive Trust confidential information is used on it.
g. Users are not permitted to store any Trust information on any equipment or portable media except that approved by the Trust, This approval list is held by ICT
h. Users are not permitted to store any Trust information on cloud storage services such as icloud, google drive, Microsoft onedrive, etc. except those approved by the Trust. This approval list is held by ICT
i. returning all SET ICT devices in the event of them leaving the Trust.as the ICT devices remain the property of the Trust

2. Users are not permitted to store personally identifiable / confidential information (such as video, music and pictures) on Trust equipment

3. aAll information created or stored on Trust equipment is deemed to be the property of the Trust.

4. Users of all Trust devices, including Corporately owned, personally enabled (COPE) devices, are only permitted to attempt to install authorised applications For example, inappropriate applications / subjects include:

- Pornography, racism, sectarianism, etc

6. Staff should be aware that devices are Corporate assets and the Trust reserves the right toremotely restore the device to factory settings, i.e. remove ALL applications and data from the device, without notice to the designated user(s).

4.0 KEY POLICY PRINCIPLES

4.1 Key Policy Statement

4.1.1 Each computer system accessed and maintained by the Trust will have a nominated System Manager who will have day-to-day responsibility for ICT Security on that system.

4.1.2 The ICT Services Manager will maintain an up-to-date Asset Register to hold details of all the items of hardware and software that make up the Trusts Information systems.

4.1.3 The ICT Business Continuity Manager is responsible for the development, testing and maintenance of an ICT business continuity plan to minimise disruption in the event of a disaster.

4.1.4 Trust staff must take all reasonable care to ensure that no information, especially Trust confidential information, is disclosed to unauthorised individuals.

4.1.5 ICT security awareness for All staff is achieved through signposting to Trust policies during induction, mandatory training (Information Governance) and from other related policies

4.1.6 Appropriate anti-virus programmes are implemented and maintained to ensure that all Trust networked PC's, servers, gateways and standalone PCs are interactively scanned for computer viruses

4.1.7 The Trust implements appropriate procedures to ensure that no illegal software is used and prevents installation of unauthorised software.

4.1.8 Trust ICT Equipment is the responsibility of each individual user, with each user being responsible for assuring that there is no inappropriate use of the equipment (including portable computers).

4.1.9 The Trust implements effective mechanisms for regularly reviewing ICT Security / ICT Security Training programme thereby ensuring that the HSC-wide network is not put at risk.

4.1.10 The Trust will co-operate with regional mechanisms established to monitor security breaches and imminent threats, reporting any IS security breaches in accordance with standard procedures.

4.1.11 Each contract of employment will have a Confidentiality and Information Security clause to reflect compliance with this ICT Security Policy.

4.1.12 Breaches of ICT Security Policy by staff may be considered to be a disciplinary matter.

4.2 PHYSICAL AND ENVIRONMENTAL SECURITY

4.2.1 Protection of Data from Unauthorised Access

Password Management

- Domain Passwords must have the following characteristics:
  - Passwords must be at least eight characters in length.
  - Passwords must contain characters from three of the following four categories:
    - English uppercase characters (A through Z).
    - English lowercase characters (a through z).
    - Base 10 digits (0 through 9).
    - Non-alphabetic characters (for example, !, $, #, %).
  - Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.

- Passwords will be changed every 90 days on all user accounts

- Users will be limited to three successive failed login attempts before the account is locked for 5 minutes.

4.2.2 Unattended computer access

Users should not leave computer equipment unattended while they are logged in without locking the computer or logging out.

If staff wish to use computer equipment which is logged in to another member of staff, that staff member should log that account out / switch user before logging on.

4.3 Internet Passwords

Passwords used by staff for any of Trust services must not be duplicated when registering with any Internet services.

4.4 Use and Management of Passwords

Passwords must not easily relate to the user or the system being used. Passwords should be chosen with care but not be so complex that they cannot be remembered by the user who is then tempted to write them down. Particularly bad examples are:

- your own or partner's name
- your pet's name (especially if you talk about your pet in work);
- your car make or registration number
- the name of your favourite sports team.

There are four simple rules for password management:

* Choose a password that cannot be easily guessed;
* Do not write your password down (including storing it in a file on your PC); NB. See Password Contingency & Shared Services below.
* Keep it a secret (except for Contingency reasons there is absolutely no reason why anyone else should know your personal password);
* Change your password immediately if you have reason to believe that it has been compromised. Any such incidents must be reported to the ITSO.

Any staff who have access to account names and/or password details of other staff as part of their normal work must never take advantage of that knowledge to access those accounts without appropriate authorisation and must never pass on that information to any others.

Failure to comply with this instruction could result in disciplinary action.

4.5 Temporary Users

There are occasions where it is necessary to set up temporary access to systems for the use of locums or other 'temporary users'. In these cases, rather than gaining access through a Trust officer's login account, a special account will be assigned to them through the use of a temporary user swipe card. The usernames/passwords on the swipe cards are set to never expire by ICT and cannot be reset by the user. It is the responsibility of the appropriate department holding these temporary cards to have a process in place to manage how they are signed out to the users and how they are returned when their duty is complete.

4.6 Password 'Cracking'

Use of password cracking software, or any other means for discovering passwords, is absolutely prohibited to all staff other than the ITSO except on the written authority of the Chief Executive each time such a facility is required.

It is not expected that such written authority will be given to staff.

4.7 General Monitoring

The ITSO and/or System Manager should carry out regular checks to confirm that all staff have implemented passwords and that the passwords are regularly changed.
Any failures to comply with the requirements of this document should be reported to Line Management who may initiate disciplinary action.

Monitoring should also include confirming that passwords and accounts for staff who have left the organisation and for consultants and others granted temporary access rights have been deleted. Checks should also be carried out to ensure that transfers of staff from team to team have also been affected at the appropriate time.

4.8 Access control to secure areas

Appropriate access / entry controls will be put in place for key ICT facilities (e.g. data centres) in order to safeguard this key resource from malicious or accidental damage (due to unauthorised access).

Areas designated as secure ICT areas are listed within and must be managed through the Procedure - secure ICT area access

4.9 Securing offices rooms and facilities

Computer rooms and communications rooms should be sited to avoid unauthorised public access. Doors and windows should be locked when unattended.

4.10 Equipment security

4.10.1 Equipment siting and protection

4.10.1.1 All users must ensure that their Trust equipment is locked or logged off when not in use.

4.10.1.2 Screens, keyboards and printers, where practicable, must be physically positioned such that they are protected against accidental disclosure of passwords or any other confidential or sensitive data.

4.10.1.3 The mobile device policy details security arrangements around this specific equipment when used on and off Trust premises. – Check mobile phone policy

4.10.1.4 All other ICT equipment should be held on Trust premises unless authorised by ICT.

4.10.1.5 Any movement of Trust devices the Trust locations must be authorised by the ICT Department prior to relocation.

4.10.2 Security of equipment off-premises

4.10.2.1 ICT equipment which is authorised for use off-site must be provided with appropriate access protection, including passwords

and/or encryption, and must not be left unattended in public places.

4.10.2.2 The user must ensure that no unauthorised person has access to the equipment. This includes access by family members.

4.10.2.3 Staff are not permitted to change any settings on ICT equipment or attempt connection to non-trust networks outside of those used for the purpose of approved remote access.

4.10.3 Network security

4.10.3.1 Staff are not permitted to connect devices / equipment to network outlets without ICT authorisation.

4.10.3.2 Suitably qualified and experienced ICT staff are appointed to manage the Trust's network and preserve its integrity in collaboration with the nominated system owners.

4.10.3.3 The Trust will adhere to the HSC Code of Connection with regard to 3rd party remote access to the network.

4.10.4 Secure disposal of equipment

Equipment owned by the Trust must only be disposed of by members of the ICT Department who have ensured that the relevant security risks have been mitigated.

4.11 Transfer of Data via Courier Services

4.11.1 Routine Courier Transfer

- Routine courier services should only be used for the transfer of non-personally identifiable or non-sensitive information only.
- Authority to use courier service must be obtained from appropriate level of management (Assistant Director or Director level).
- Contact ICT service desk to facilitate the process for transfer of electronic data via courier services

4.11.2 Secure Courier Process

- Secure courier services should always be used for the transfer of personally identifiable or sensitive information.
- Authority to use courier service is obtained from appropriate level of management (Assistant Director or Director level).
- Contact ICT service desk to facilitate the process for transfer of electronic data via courier services

4.12 Electronic Transfer of Information

All sensitive information electronically transferred outside of the HSC network must use Trust Email. An email encryption Guide is available on iConnect.

4.13 Security Incidents

4.13.1 Details of all real or suspected ICT security incidents must be reported immediately to the ICT Service Desk and an Incident Report Form submitted to ICT. Such details will also be passed to the HSC ITSO as appropriate.

4.13.2 ICT Security incidents will be properly investigated with associated evidence being formally collected, recorded and processed. ICT security incidents may also need to be reported to external organisations e.g. PSNI or Information Commissioner. These referrals will be undertaken by authorised persons such as the ICT Services Manager, Assistant Director of Technology & Telecoms.

4.13.3 Users/staff of ICT services are required to report any observed security weaknesses in, or threats to, ICT systems. The weaknesses should be reported to the ICT Service Desk. Users should not, in any circumstances, attempt to prove a suspected weakness as this will be interpreted as potential misuse of the system. Where appropriate users should also inform their line manager.

4.14 Protection from malicious software

4.14.1 Virus controls

The deliberate introduction of malicious software to a system is a criminal offence under the Computer Misuse Act 1990. However the most likely introduction of viruses will be through illegal software, email or outside contractors. The following action points should be used as a basis for virus control.

- No files will be loaded on to any system from CD/DVD, USB drives unless they have first been virus checked. All workstations, networked or stand-alone (including remote users) will be provided with utilities to virus scan all files before they are opened. This includes diagnostic software run by outside support engineers.
- USB Drives being used to send files to other users will be virus checked before they are sent. This also includes all files saved as attachments and sent via email. Anti-virus software is installed on all end user devices where appropriate to facilitate this.
- All networked computers and servers will utilise Anti-virus software which will be updated automatically with appropriate releases.
- Where a virus is detected this must be reported immediately to the ICT Service Desk who will log the incident and deal with it accordingly,
- The Trust will apply software patches to all vulnerable computer systems after due consideration of the associated risks.

4.15 Protection of Hardware from Theft

4.15.1 Access to specific areas of the ICT Department is restricted to authorised personnel only with electronic access controls in place to restrict unauthorised physical access where appropriate.

4.15.2 The Trust Data Centres must always be kept locked when not in use.

4.15.3 Keys to the Trust Data Centres must be clearly marked and kept in a secure location.

4.15.4 ICT Comms cabinets should always be kept locked with the keys to be kept in the ICT Department.

4.15.5 Hardware in particularly vulnerable areas or containing sensitive data should make use of available physical security measures such as locking offices or chaining hardware to desk.

4.15.6 Alarms must be enabled out of hours where they are present.

4.15.7 Redundant hardware must be returned to the ICT Department. Staff are responsible for identifying such equipment and returning to ICT Department.

4.16 Protection of PCs (USB Ports)

- Only approved, encrypted USB Storages devices may be used with Trust Equipment.
- Access to all non-approved USB Storage devices is actively blocked on Trust equipment.
- Appropriate centrally administered software is deployed which manages all aspects of USB ports including authorisation of use of USB drives by designated users.
- Trust data must not be held on a USB storage device for longer than is necessary. These devices should be regarded as a means of transporting data and not as the primary means of storing data.
- Data on Trust USB storage devices must not be copied onto personal devices
- Theft, loss or damage to the device or the data held must be reported to line management and the ICT Department immediately. If necessary a SET Incident Report Form (IR1) should be completed.

4.17 REMOTE ACCESS

4.17.1 Remote Access is made available by the ICT Department to maximize the benefits of Information Communication Technology.

4.17.2 A Remote Access Request form must be completed and approved by the appropriate level of management to support the application for Remote Access (refer to Trust Intranet for the appropriate form).

4.17.3 In circumstances where the Trust approves remote access to the Trust ICT Systems to fulfil an operational need the Trust may provide the appropriate ICT equipment and services.

4.17.4 Staff using portable computers must take all reasonable steps to guard against their theft, loss, damage and unauthorised use. Special consideration should be made when travelling as they will be more open to theft and physical damage. Laptops must not be left in a car or any other place where they would be visible to a thief.

4.17.5 Participating staff must comply with GDPR, Personally identifiable / Trust confidential data processed outside a Trust location should be protected to the same level as it would be in a Trust workplace. (The location of processing does not alter the responsibility on the individual to keep the data secure. The Trust's policy and procedures regarding confidentiality of information must be maintained.

5.0 IMPLEMENTATION OF POLICY

5.1 Dissemination

This policy will be brought to the attention of all staff. Staff provided with Trust mobile phones/devices are fully aware of the provisions of this policy.

This policy will be posted on the Trust Intranet site.

5.2 Resources

All staff in receipt of a mobile phone / device will be made aware of this policy.

5.3 Exceptions

Not Applicable

6.0 MONITORING

The Assistant Director Technology & Telecommunications shall monitor compliance to this policy via appropriate Trust Systems and associated practice.

Failure to comply with this policy may result in disciplinary action.

7.0 EVIDENCE BASE / REFERENCES

Code of Confidentiality for Protecting Service User Information
General Data Protection Regulations (GDPR)

8.0 CONSULTATION PROCESS

Not Applicable

9.0 APPENDICES / ATTACHMENTS

Appendix 1: Guidance for System Managers

10.0 EQUALITY STATEMENT

In line with duties under the equality legislation (Section 75 of the Northern Ireland Act 1998), Targeting Social Need Initiative, Disability discrimination and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.
The outcome of the Equality screening for this policy is:

Major impact ☐

Minor impact ☐

No impact. ☒

SIGNATORIES

(Policy – Guidance should be signed off by the author of the policy and the identified responsible director).

Form Status	Policy Name	Author Endorsement	Modified	Modified By
Directorate	ICT Security	Yes	16/04/2015 04:47 PM	Stewart, Stephen

Form Status	Policy Name	Approval	Modified	Modified By
Read Only	ICT Security	Endorsed	23/04/2015 12:48 PM	Coulter, Roisin
Read Only	ICT Security	Endorsed	15/12/2015 03:25 PM	McCaughey, Hugh

Appendix 1

Guidance for System Managers

Date: _____

Completed by: _____

Have You.....	Yes	No	Not Possible	Comments
An appropriate process for users/managers to **request a new account** for **new staff**?				Can be included in local Induction
An appropriate process for users/managers to **request a new account** for **a Third Party or other non-Trust individual**?				
An appropriate process for **changing user access** rights for **staff, Third Parties and other non-Trust individuals**?				
An appropriate process for **obtaining leavers** information?				
An appropriate process for **disabling/removing leavers** accounts? (Note: you will need to understand the impact that removing an account will have (if any) on historical data).				
An appropriate process for **creating a new account** and assigning permissions for **Third Party or other non-Trust individuals**?				
Generic or Group accounts?				
Defined user access privileges based on role/function?				
System Timeouts set (as appropriate)?	Y			Set by ICT group policy
An audit trail of user access logs?				
A Data Access Agreement in place for all Third Parties who have access to Trust information (potential or actual) or contract with the supplier?				
A process implemented to regularly review all Third Party accounts to ensure they are still required?				
Standard monitoring procedures documented, agreed and communicated to user group, including informing IAO of suspected or actual information breaches?				
Implemented standard monitoring procedures (as agreed and documented above)?				
A documented “User Guide” for new users?				
A formal process for communicating with system users?				