Belfast Health and Social Care Trust
caring supporting improving together

Reference No: BHSCT/ICT (01) 2021

Title:	**ICT Security Policy**		
Policy Author(s)	Jill Nicholson, ICT Governance & Security Manager [redacted] jill.nicholson@belfasttrust.hscni.net Gillian Acheson, Senior Manager Data Protection [redacted] gillian.acheson@belfasttrust.hscni.net		
Responsible Director:	Charlene Stoops, Director of Performance, Planning & Informatics		
Policy Type: (tick as appropriate)	*Directorate Specific ☐	Clinical Trust Wide ☐	Non Clinical Trust Wide ☒
If policy type is confirmed as ***Directorate Specific** please list the name and date of the local Committee/Group that policy was **approved**			
Date:			

Approval process:	Trust Policy Committee Executive Team Meeting	**Approval date:**	01/04/2021 14/04/2021
Operational Date:	April 2021	**Review Date:**	April 2026

Version No.	3	**Supercedes**	V2 – September 2017 – September 2022

Key Words:	ICT Security
Links to other policies	Standard 1 - Procurement incl Contract Management of IT (digital) Hardware, Software, Systems or related Services BHSCT Policy on data protection and protection of personal information (2018) TP 26/08 BHSCT Records management policy (2018) TP 13/08 BHSCT Records retention and disposal schedule (2018) TP 14/08 BHSCT Policy on the access to data for organisations external to the Trust (2018) TP 69/10 BHSCT Social media policy (2019) TP 76/11 BHSCT Transportation of records policy (2018) TP 85/13 BHSCT Medical device policy and associated procedures (2017) TP 16/08 BHSCT Adverse incident policy (2020) TP 08/08 BHSCT Disciplinary policy (2015) TP 52/08 BHSCT Fraud policy statement (2017) TP 63/10 BHSCT Risk management strategy 2020 – 2021 TP 58/08 BHSCT Business Continuity Management Framework V2 Jan 2015 HSC ICT Security Policy V1.19 NI Public Procurement Policy V11 Aug 2014 and associated Procurement Guidance Notes (PGNs)

Date	Version	Author	Comments
25/03/2009	0.1	J Nicholson	Drafted
02/08/2017	1.0	J Nicholson G Acheson	Policy Committee approval
09/08/2017	2.0	J Nicholson G Acheson	Policy Committee approval
01/04/2021	3.0	J Nicholson G Acheson	Policy Committee approval

1.0 INTRODUCTION / SUMMARY OF POLICY

1.1 Background

The data stored and processed within our computer systems, stand-alone and networked, represents one of the Trust's most valuable assets. It is essential that all ICT within the Health and Social care environment are protected to an adequate level from all likely events which may jeopardise our business activities.

The General Data Protection Regulation (EU 2016/679) and Data Protection Act (2018) define the legal basis for UK organisations to take steps to ensure that personal data is adequately protected by placing a legal obligation on them to do so. In addition, the Network and Information Systems Directive (EU 2016/1148) and Network and Information Systems Regulations (2018) establish the legislative framework that governs the security of essential network and information systems.

Within the Trust information system users handle information which may be potentially sensitive and, on many occasions highly confidential. All Trust staff who develop, operate, maintain or use ICT have an explicit and legal obligation to preserve the security of those systems.

The policy statement and associated guidelines aim to provide direction in relation to safeguarding the integrity and confidentiality of information held on the Trust's computers. As we move further towards sharing information electronically with external bodies, it is essential that we ensure its integrity and confidentiality.

1.2 Purpose

The purpose of this policy is to protect Belfast Health and Social Care Trust (BHSCT) information assets from all threats whether internal, external, deliberate or accidental.

This document provides a framework for security of all Information and Communication Technologies (ICT) in use throughout the Trust.

All other policies, procedures and standards operate under the context of this policy, including where individual systems may already have developed a security policy specific to its individual system policies.

1.3 Objectives

The guidance in this document aims to ensure that:

- ICT used in the Trust is properly assessed for risks and threats to security
- Appropriate levels of security are applied to maintain the confidentiality, integrity and availability of Information and ICT
- All staff are aware of their roles, responsibilities and accountability for information security

- A means is established to communicate awareness of information security issues, their impact on the organisation for management, users and other staff.
- Procedures to detect, investigate and resolve security breaches are in place and are dealt with consistently throughout the Trust.
- Relevant legislation and regulatory requirements are complied with.
- Plans are in place to ensure business continuity for all business critical systems.
- Monitoring arrangements exist to audit the ongoing effectiveness of the information security arrangements in the Trust.

2.0 SCOPE OF THE POLICY

This policy applies to:

- All parties who have access to, or use of ICT Systems and Information belonging to, or under the control of, BHSCT, including:
  - BHSCT employees
  - Other Health & Social Care (HSC) employees
  - Temporary Staff including agency/bank staff
  - Volunteers
  - Third Party Contractors
  - Any other party making use of BHSCT ICT resources
- Information stored, or in use, on BHSCT ICT Systems;
- Information in transit across BHSCT protected network;
- Information leaving the BHSCT protected network;

This policy also applies equally to both corporate and non-corporate devices used to process Trust information, including medical devices.

3.0 ROLES AND RESPONSIBILITIES

3.1 Chief Executive Officer

The Chief Executive is responsible to the HSCB for the secure operation of ICT & Information Systems within BHSCT.

Responsible for:

- Ensuring a nominated officer with sufficient authority is appointed to ensure security related matters are adopted throughout the organisation.
- Ensuring frameworks are in place to ensure information systems are appropriately assessed for security and protected in accordance with this policy, including ensuring System Managers are identified for each information system.
- Ensuring the organisation maintains compliance with HSC ICT Security Policy
- Ensuring clear policy direction is set and management demonstrate support for and commitment to information security across the organisation and regionally.

3.2 Senior Information Risk Owner (SIRO)

Responsible to the Chief Executive, advising on the information risk aspects of his/her statement on internal controls.

Responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs
- Owning the organisation's information incident management framework.

3.3 Information Asset Owners (IAO)

Responsible to SIRO, providing assurance that information risk is being managed effectively in respect of the information assets that they 'own'.

Responsible for:

- Identifying all the information assets within their area of responsibility
- Knowing what information comprises or is associated with an asset, and understands the nature and justification of information flows to and from the asset
- Knowing who has access to the asset, why they have access, ensuring access is compliant with all appropriate policies, procedures or standards.
- Understanding and addressing risks to the asset, and providing assurance to the SIRO
- Ensuring appropriate information assurance is in place and managed for 3rd party organisations who have access to Trust information/assets eg via contracts, data sharing agreements etc.

3.4 ICT Security Officer/Manager

Responsible to Co-Director IT & Telecommunications, providing a local focus on all ICT Security matters.

Responsible for:

- Co-ordinating ICT security matters across departmental and system boundaries within the organisation
- Taking the lead in implementing and monitoring the effectiveness of ICT security policy, procedures, standards, guidelines within the organisation
- Taking a pro-active role in establishing and implementing an ICT Security Programme including training, awareness and guidance
- Promoting ICT Security Awareness across the organisation, including compliance with relevant legislation including General Data Protection Regulation (EU 2016/679), Data Protection Act (2018) and Network and Information Systems Regulations (2018).

- Receiving and considering reports of ICT Security incidents from System Managers or others, ensuring the necessary corrective or preventative actions are implemented
- Liaising with the NIS (2018) Regulator, the Competent Authority, with regards to reportable incidents
- Liaising with HSC ICT Security Manager on matters of ICT Security which may impact other HSC NI organisations.
- Representing the organisation on HSC-wide security groups/forums

3.5 System Managers

Responsible to Information Asset Owners ensuring that information security requirements, expectations and limitations are mutually understood and agreed, and processes are in place to securely and effectively manage the day to day operations of BHSCT information systems.

Responsible for:

- Day to day operational management of the information system including implementation of suitable measures to ensure system is secure, including regular review of the same to ensure they remain up to date.
- Working in conjunction with ICT department to ensure core local processes are consistently applied across all information systems
- Ensuring users of the system are appropriately trained in relation to the security of the system.
- Prompt reporting of security matters/breaches to the ICT Security Officer/Manager.

3.6 All Users

Responsible for:

- Complying with all local and regional ICT & Information Security Policies, procedures or standards
- Ensuring attendance at all necessary ICT & Information security awareness/training sessions
- Reporting adverse incidents relating to ICT or Information security in accordance with local policies, procedures or standards.
- Reporting weaknesses in operating/security procedures in accordance with local policies, procedures or standards.

3.7 Special Interest Groups

ICT Security Manager is nominated to co-ordinate in-house knowledge and experiences to ensure consistency and provide help in ICT security decision making.

ICT Security Manager will be provided with access to suitable external advisors to provide specialist advice outside their own experience. Examples of these Special Interest Groups would be CLASS and CHECK consultants (www.ncssc.gov.uk)

4.0 CONSULTATION

IT & Telecommunications Senior Management Team
Digital Steering Group
Information Governance Board, Cybersecurity Subgroup
Trade Unions

5.0 POLICY STATEMENT/IMPLEMENTATION

5.1 Policy Statement

The Chief Executive, through appropriate forums such as the Digital Steering Group and Information Governance Board, is committed to ensuring that information security is given the highest possible degree of importance. Information is central to our business and it is our aim to ensure that the confidentiality, integrity and availability of this information is protected at all times.

We will ensure that we continually identify and assess the threats to information security with which we are faced and will develop controls and systems that are aimed at controlling such threats and minimising the risk of information security breaches.

In support of this policy we have developed specific standards, policies and procedures aimed at the management of information security. All staff have a specific responsibility for ensuring that the requirements of these policies are adhered to and all staff will receive training in relation to these policies and procedures.

All users should use their best efforts to adopt industry best practice in its procedures for the maintenance of information security and in particular the recommendations and guidelines for security management standards contained within International Standards ISO27001 and ISO20000.

The ICT Security Manager is responsible for implementation of the ICT Security Policy and procedures. However all Trust users have responsibilities for the security and safety of Trust ICT systems and the information held on the systems. All users are to be made aware of the policies and procedures set out in this document. Each user is responsible for maintaining system security to the extent laid down in this document.

This policy, with approval from the appropriate forums such as the Information Governance Board and Digital Steering Group, may be altered when required to reflect changes to the configuration of its systems and applications and to ensure continued compliance with statutory and other legal requirements. Users will be notified of any material changes to this ICT policy.

5.2 Organisation of ICT Security across BHSCT

5.2.1 Co-ordination

BHSCT co-ordinates strategic ICT Management through a Digital Steering Group co-chaired by the Director of Performance, Planning & Informatics and the Director of Nursing and User Experience, with representatives from across all Directorates/Divisions and HSCB eHealth Team.

BHSCT co-ordinates Information Governance management through an internal Information Governance Steering Group (Information Governance Board) chaired by the Senior Information Risk Owner (SIRO). A number of subgroups, including a Cybersecurity Working Group, support this group.

5.2.2 Operational Management

BHSCT is responsible for implementing a local programme of ICT & Information Security management, including the provision of necessary skills, training and resource to ensure adherence to this policy.

This will be achieved through regular Digital Steering & Information Governance Board management meetings which include the discussion of ICT & Information Security matters and controls.

5.2.3 Collaboration

BHSCT ICT & Information Governance Services will work closely together with all other Service Areas to ensure the successful implementation and development of ICT & Information Security across the Trust.

BHSCT Service Areas should seek appropriate advice and guidance from ICT & Information Governance services before undertaking any new projects or changes which may impact ICT or Information Security to ensure risks are identified at any early stage and appropriate direction undertaken.

BHSCT will work with other HSC organisations to ensure the successful implementation and development of ICT & Information Security across NI Health & Social Care. This includes active participation in Regional Forums / Groups including the HSC ICT Security Forum, and Information Governance Advisory Group(IGAG).

5.2.4 Core Infrastructure

IT & Telecommunications Department provides and maintains the central ICT infrastructure for BHSCT.

5.3 Policy Principles

Information & ICT Services are provided by BHSCT in order to assist users in the performance of their role.

All access to Information & ICT Services provided by BHSCT is regarded as business use and subject to the terms outlined in this policy.

All information held on all BHSCT systems is considered to be confidential and the property of Belfast Health & Social Care Trust.

All use of BHSCT ICT & information systems will be electronically logged and may be monitored in accordance with all appropriate legislation and guidance.

5.4 Acceptable Use

All users of BHSCT ICT Systems and Information must abide by the terms of the ICT Security Policy, associated standards, codes of conduct and appropriate legislation.

5.4.1 Email System

BHSCT provides a corporate Email System to assist all staff in the performance of their duties.

Any email messages sent & received will be treated as business messages.

Staff must use the Trust Email System (or other agreed secure system [redacted]) for the communication of Trust business.

Emails containing sensitive information should be suitably secured in line with the BHSCT Policy On the Data Protection Act and Protection of Personal Information and associated guidance[1]. Technical solutions [2]for both file & email encryption are available to staff.

Service Groups should consider the appropriateness of email communication with patients/clients and must have made adequate risk assessment prior to introduction.

BHSCT Managers can access individual emails, if necessary, when staff members are not available in order to ensure continuity of service.

5.4.2 Email Filtering System

BHSCT has the right to block incoming and outgoing emails to preserve the integrity of its systems.

BHSCT has an email filtering system in place which will prevent some emails from reaching/leaving the Email System, such as spam, files of malicious intent and where content is regarded as inappropriate.

A release process via ICT has been implemented for business correspondence which may have been filtered in error.

[1] See "Guidance on transferring information securely" [redacted]

[2] Up-to-date information on technical encryption solutions is available [redacted]

5.4.3 Email Archive

All emails generated in the course of BHSCT business are potentially discoverable under Freedom of Information Act, General Data Protection Regulation (GDPR) and Data Protection Act 2018.

BHSCT has an email archive solution in place, [redacted]

Individual account holders have access to search the archive for emails they have sent or received.

Wider searches of the mail archive are restricted to authorised ICT personnel only on receipt of an appropriately authorised request.

5.4.4 Internet

BHSCT provides limited access to the Internet for its staff primarily to assist them in the performance of their duties.

Access to restricted sites will only be granted following authorisation of a BHSCT Senior Manager, and where access has been suitably risk assessed.

Personal Use of Trust Internet is permitted provided access:

1. Is reasonable & occasional
2. Is carried out in an employee's own time & does not interfere with other staff carrying out their work duties
3. Is not used to facilitate private business or other commercial interests
4. Does not result in personal financial gain
5. Is compliant with Trust/HSC policies on standards of business conduct
6. Does not result in employees entering into contractual agreements on behalf of BHSCT unless authorised to do so.

BHSCT will not accept liability for any financial loss while using BHSCT systems for personal transactions.

BHSCT logs all Internet access by individuals and reserves the right to access and report on this information to ensure compliance with this policy.

5.4.5 [redacted]

BHSCT provides [redacted] as a basic conversation & communication tool, primarily to assist staff in the performance of their duties. [redacted]

[redacted] should **not** be used for formal business communications such as:

- conversations where decisions may be sought/made;
- where cases may be discussed;
- where person identifiable or sensitive information is divulged;
- where business collaboration occurs or documents are exchanged.

All use of [redacted] will be treated as business use.
[redacted]

5.4.6 Social Media

Use of social media may subject employees to disciplinary action if personal information or views of BHSCT cannot be isolated from professional views.

BHSCT provides access to social media sites for authorised staff to assist them in the performance of their duties.

BHSCT ICT equipment or systems must only be used to access or update BHSCT related Social Media sites, not personal sites.

5.4.7 ICT Equipment

BHSCT provides ICT equipment for business purposes.

All ICT equipment, and the data contained therein, remains the property of BHSCT.

All ICT equipment must be used in accordance with the stated policies, associated standards, codes of conduct, appropriate legislation, and returned to BHSCT when employment or contract ceases.

ICT Department will provide access to all necessary software via central management tools.

Users are not allowed to make personal and unauthorised modifications to hardware and/or software on BHSCT ICT equipment.

Data should only be processed and stored using approved Trust ICT equipment, systems and software.

5.4.8 Passwords

Authorised access to BHSCT networks will be granted in the first instance by means of a unique identifier. In most cases this will be [redacted]

Additional security may be used to prevent unauthorised access to specific ICT systems.

The use of generic accounts will only be permitted in exceptional circumstances, [redacted]
Such accounts must be authorised by IAO following suitable risk assessment and consideration of all other options.

Users **must not** share passwords. The user will be held responsible for any activity on their account.

5.4.9 Human Resources Security

Terms & Conditions of Employment

All BHSCT contracts of employment must include statements requiring compliance with ICT & Information Security policies & procedures.

All managers should ensure that roles with specific responsibility for security of assets or information are included in job definitions, including employees, contractors and third parties.

5.4.10 Screening / Vetting

Screening and elevated security vetting may be required for roles which relate directly to sensitive security matters or access to highly sensitive data.

Screening and vetting must be carried out in accordance with HR policies and procedures.

5.4.11 Third Party Access

Third party access to BHSCT ICT & Information must be controlled in order to maintain the necessary levels of physical and logical security, and subject to appropriate contracts/data access agreements or Statements of Compliance[3].

IAOs must ensure that ICT & Information Security clauses, particularly with regards to General Data Protection Regulation, Data Protection Act (2018) and Network and Information Systems Regulations (2018), are built into all formal service contracts.

Third Party remote access should only be via agreed and secure connections. (3rd party access request form available on the Hub)

5.5 Access Control

5.5.1 Account Management

All System Managers must ensure that procedures are in place to manage access to ICT & Information systems, by way of individual user accounts. User Account Procedures must also manage changes when users are transferred to other roles and removals when a user leaves.

Security Privileges and access rights must be allocated based on the requirements of a user's role and should be consistent across all areas.

5.5.2 Authorised Use

Access to BHSCT ICT Systems and Information is only permitted where the access is required to support BHSCT areas of business or associated service.

[3] See Appendix I – 3rd Party Statement of Compliance

Access to BHSCT ICT systems is restricted to authorised personnel only. These may include staff, contractors, Third Party suppliers and temporary staff.

New and existing users will only have access to BHSCT business applications if they have been authorised by an appropriate manager.

5.5.3 Staff Remote Working

From time to time, staff may need to access the Trust network from locations other than their office (e.g., from home).

All remote access to HSC information systems from outside BHSCT protected network must be subject to [redacted]

Staff Remote access should only be through [redacted] (Staff Remote Access request form available [redacted])

5.5.4 Software Management (incl Antivirus / Patching)

All users must ensure they do not engage in any action which may result in the introduction of malicious software e.g. using external files, downloading files from the Internet.

All System Managers must ensure that they have a software maintenance routine in place, patching and updating vulnerabilities regularly in order to minimise the associated threats.

Where this function is carried out by the ICT Department, System Managers are responsible for reporting any errors or exceptions to the ICT Service Desk.

All new ICT equipment and systems purchased should be capable of being patched and updated regularly.

"End of Life" software which is still required should be replaced with a supported version or alternative solution based on a risk assessment of the specific environment.

5.6 Procurement Lifecycle incl Asset Management

5.6.1 System Lifecycle

ICT Security must be considered at the beginning of any procurement or development of information processing facilities, and at key changes/stages along the lifecycle thereafter, building in appropriate authorisation mechanisms.

5.6.2 Procurement & Contract Management

Procurement of digital hardware, software, systems or related services must only be progressed where the purchase:

- is deemed suitable for the agreed purpose

- has suitable funding allocated and approved by the relevant authority
- is not counter-strategic to either the eHealth Digital Strategy or Trusts Digital Strategy or Plan
- will conform to the Trusts minimum technical and security standards
- has a realistic prospect of delivery, invoice and payment within the given financial year.

All aspects of the Procurement Lifecycle for digital hardware, software, systems or related services (including commissioning, purchasing leading to contract award, and contract management) must:

- Comply fully with all relevant legislation, regulations and Trust Standing Financial Instructions
- Operate in accordance with Procurement Control Limits (PCL) and thresholds
- Operate in accordance with the Twelve Principles Guiding Public Procurement in Northern Ireland
- Ensure management of conflicts of interest as set out in the Trusts Procurement Guidance

All LIVE contracts associated with digital hardware, software or systems must be recorded [redacted].

All purchases of ICT equipment must be funded from Trust Capital funds, unless otherwise authorised by the Director of Finance.

All ICT equipment and software requests must be processed through the ICT Department.

It is the responsibility of budget holders and contract managers to monitor expenditure against contract.

5.6.3 Asset Management

Information Asset Owners are appointed with responsibility for each logical or physical set of assets.

IAOs are responsible for maintaining an inventory of their information assets which will be managed in accordance with the relevant policies, standards, codes of conduct and legislation. This inventory must be managed to include updates when assets are transferred to other individuals or returned when an individual is leaving or a contract is terminating.

IAOs should ensure that procedures are in place to ensure that information or information assets are not taken / transferred off-site without management authorisation.

5.6.4 Asset Disposal

Where an asset has ever been used to process personal data (as defined under the General Data Protection Regulation (GDPR)/Data Protection Act

2018) or sensitive/confidential data then the asset must only be disposed of after reliable precautions to destroy the data have been taken, in accordance with the ICT Disposal Standard.

A. Digital Devices/Information

Only the ICT Department are authorised to identify ICT equipment/media as no longer fit for purpose and for disposal.

All ICT equipment that has been provided by external suppliers for projects or evaluation should be securely wiped before returning to the 3rd Party, in accordance with the ICT Disposal Standard.

Disposal of information or information assets carried out by a Third Party MUST be carried out under the relevant HSC contract for the secure collection, erasure/destruction and disposal services for ICT and miscellaneous Electronic Equipment.

B. Non-Digital Devices/Information

All confidential or sensitive information held in non-digital forms (paper, film etc) should be shredded, burnt or pulped.

Disposal of non-digital information carried out by a Third Party MUST be carried out under the relevant HSC contract for the collection, shredding/destruction and safe disposal/recycling of confidential paper and optical/magnetic material.

5.6.5 Removable Media Handling

The use of removable media/devices for BHSCT business is not taken lightly due the risks associated with the need for secure storage of data. Reasonable justification has to be provided that there is an absolute business requirement for the use of such a device, with no other more secure alternative available.

Every effort should be made not to store confidential or business sensitive information on removable media/devices.

All removable media containing confidential or sensitive information MUST be encrypted, in accordance with the appropriate encryption standard[4], prior to removal from secure trust premises.

All staff MUST ensure that use of such devices is strictly limited to those circumstances which have been authorized, and information is transferred to BHSCT network as soon as possible.

[4] See "Encryption standards guidance" [redacted]

5.6.6 Secure Printing

BHSCT have a large printer fleet, [redacted] to accommodate a wide range of printing needs.

Where printing involves sensitive information, staff must take extra care to ensure the printouts are not sent to the wrong printer, including the use of secure printing facilities where they are available[5].

5.6.7 Physical & Environmental Security

All System Managers/IAOs must ensure that processes are in place to consider physical security and controls relative to the value and risk of ICT Systems & Information within those physical boundaries. [redacted]

5.6.8 [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

5.6.9 External Hosting (incl Cloud Computing)

External hosting of systems, including cloud computing, are models for enabling on-demand access to computing resources (eg networks, servers, storage, applications and services) from multiple locations. However there are a number of specific risks that need to be addressed to ensure that suitable levels of protection are applied to BHSCT data and information.

Where data is being hosted external to the BSHCT protected network information-based risk assessments[6] should be carried out, [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[5] See "Good Practice Printing Guidelines" available [redacted].

[6] See "External Hosting Risk Assessment Guidance" available [redacted].

- [redacted]

[redacted]

[redacted]

It is recommended that technical risk assessments are carried out as appropriate, to provide the necessary technical assurances with regards to the security of the information.

5.7 Data Management

5.7.1 Data Downloads

Unauthorised subsets of any of the Trusts databases must not be:

- Downloaded without written permission of the appropriate Information Asset Owner
- Unencrypted.

5.7.2 Information Sharing

A. Personal Data (as defined under General Data Protection Regulation (GDPR))

Personal data held in HSC information systems are safeguarded by the General Data Protection Regulation (EU 2016/679) and Data Protection Act (2018) which place obligations on those who record or use such information. In addition, health professionals have ethical duties to maintain the confidentiality of data relating to their patients or clients.

The *Code of Practice on Protecting the Confidentiality of Service User Information* document issued by DHSSPS in January 2012 provides guidance on the handling of personal information.

Where formal service contracts are either absent or do not adequately cover the sharing of person identifiable data between HSC organisations and/or outside organisations, the BHSCT Data Access Policy must be followed.

B. Business Sensitive Data

Exchanges of business sensitive information (e.g. financial, contractual, proposed /planned service changes, ICT technical configuration information) should be strictly controlled.

---

[7] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

[8] See https://www.ncsc.gov.uk/guidance/cloud-security-collection

IAOs should ensure exchange protocols are agreed and implemented to ensure sensitive BHSCT information is not passed to unauthorised parties.

C. Data Retention

All data and files, including electronic, generated in the course of Trust business must be retained in accordance with DHSSPS Good Records Good Management Guidance (2012).

5.8 Governance/Compliance

5.8.1 Risk Analysis & Management

All staff must ensure that risks to the security of ICT and Information are identified, assessed, recorded on a risk register and managed in accordance with BHSCT Risk Management Strategy.

Each programme of protective countermeasures, planned to reduce the risks to acceptable measures, should be monitored and reviewed on an annual basis to ensure the programme is still relevant and that any outstanding work is being progressed.

5.8.2 Incident Reporting & Management

An information security breach is defined by ISO/IEC TR 18044;2004 as “an identified occurrence of a system service or network state indicating a possible breach of information security policy or failure of safeguards”

An information security incident is an event that has a high probability of compromising the business operations or other information security impact. An information security weakness is the potential for an information security incident to occur that was previously unknown or not considered during a risk analysis.

Both information security incidents and weaknesses are considered breaches and have potential to affect confidentiality, integrity and availability of information therefore:

- It is the responsibility of all BHSCT Employees to report actual or suspected non-compliance in line with the Trusts Adverse Incident Policy.
- All relevant parties such as ICT Security Manager, Data Protection Manager, System Managers and IAOs should maintain contact lists with key Third Parties such as law enforcement authorities, regulatory bodies, Information Service Providers, Telecomms Providers etc to ensure that advice can be obtained and action taken quickly in the event of a security incident.

5.8.3 Business Continuity

All service areas must ensure that business impact assessments and Business Continuity Plans are produced for all mission critical information, applications, systems and networks in order to maintain adequate levels of

BHSCT services in the event of any significant disruption to ICT or Information services.

These Business Continuity Plans should be subject to regular review, testing and update as necessary.

5.8.4 Disaster Recovery

[redacted].

System Managers and IT & Telecommunications Department must ensure that they have developed, and maintain Disaster Recovery plans in order to ensure the least possible disruption to critical services in the event of any significant disruption to facilities or services.

Backup and Recovery processes should be subject to a schedule of testing.

5.8.5 Audit / Independent Assurance

BHSCT is required to achieve and maintain substantive compliance in ICT & Information Management Controls Assurance Standards, in order to provide routine assurance that ICT & Information security is being effectively managed.

BHSCT will also consider a range of independent assurances including reviews by internal audit functions or by Third Party organisations specialising in such reviews, adherence to relevant industry standards eg ISO/IEC27001, or independent technical assessments to provide assurance that working practices and technical implementations properly reflect the policy and the policy is feasible and effective.

5.9 Implementation of Policy

ICT Security Manager and ICT Security Officer are responsible for actively managing ICT Security risk to BHSCT by ensuring adequate controls and a functional security management system is in place.
The ICT Security Manager will review the security risk status of BHSCT on an ongoing basis to ensure that risks are adequately being identified and managed.

5.10 Dissemination

Issue to all Trust staff via Corporate Email Notice.
Issue to all IAOs for onward issue to staff & associated 3rd Parties.
Additional communication via News Article [redacted]

5.11 Resources

This policy will be [redacted] communicated to staff in Corporate Induction and Information & IT training sessions and provided to 3rd Parties requesting remote access as part of the sign-up process.

5.12 Exceptions

No exceptions apply.

6.0 MONITORING AND REVIEW

It is the responsibility of the ICT Security Manager to maintain and review this policy on at least a triennial basis.

7.0 EVIDENCE BASE/REFERENCES

Some of the issues of ICT security are governed by legislation, and steps must be taken to ensure the Trust's compliance with relevant requirements. Currently the legislation includes but is not limited to:

a) **Civil Contingencies Act (2004):** This Act provides the framework for civil protection in the UK, and includes the need to ensure development and testing of disaster recovery and fall back contingency plans where computerised information services may be disrupted.

b) **Civil Evidence (NI) Order 1997:** This Order provides the legal basis for the use of documents and records of any format to be admissible as evidence in civil proceedings. This includes electronic patient records.

c) **Computer Misuse Act (1990):** This Act cites unauthorised access to any computerised system and the introduction of malicious software as criminal offences.

d) **Copyright, Designs and Patents Act (1988):** Section 16 of this Act states that the copyright owner has exclusive rights to the software making it a criminal offence to copy or load any licensed software.

e) **Data Protection Act (2018):** Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against loss of personal data.

f) **Electronic Communications Act (NI) (2001):** This Act makes provision to facilitate the secure use of electronic communications and electronic data storage.

g) **Environmental Information Regulations (EIR) (2004):** The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities

h) **Fraud Act (2006):** The Fraud Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position.

i) **Freedom of Information Act (2000):** Defines the right of access to information held by Public Authorities.

j) **General Data Protection Regulation (GDPR)** (**2018)**: This is a regulation by which the European Parliament, the Council of European Union and European Commission intend to strengthen and unify data protection for all

individuals within the European Union. It also addresses the export of personal data outside the EU.

k) **Health & Safety at Work (NI) Order (1978):** Defines the need to secure the health, safety & welfare of person at work.

l) **Health & Safety (Display Screen Equipment) Regulations (NI) (1992):** Defines the extent to which organisations must ensure workstations meet the requirements of the schedule, the environment is appropriate and software/systems are suitable for the task.

m) **Human Rights Act (1998):** Defines the right to personal privacy.

n) **Lawful Business Practice Regulations (2000):** Defines the purpose for which organisations can lawfully monitor and/or record communications which are transmitted by its telecommunication systems such as telephone, email and access to the Internet.

o) **Network and Information Systems Regulations (2018):** This is the legislative framework that governs the security of essential network and information systems. Defines the need for organisations such as Belfast Trust to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems, and to prevent and minimise the impact of incidents affecting the security of the network and information systems, with a view to ensuring the continuity of those services.

p) **Obscene Publications Act (1958 & 1964):** Defines the law for preventing the publication for gain of obscene matter and the publication of things intended for the production of obscene matter.

q) **Police and Criminal Evidence (NI) Order (1989):** Defines the need to determine the proper operation of computer systems from which information is used as evidence in criminal legal proceedings.

r) **Privacy and Electronic Communications (EC Directive) Regulations 2003:** Defines the law preventing the sending of direct marketing to someone who has not specifically granted permission (via an opt-in agreement) unless there is a previous relationship between the parties.

s) **Public Contracts Regulations (2006):** Defines procedures that must be followed when awarding public sector contracts for the delivery of capital projects or for the provision of goods and services.

t) **Public Procurement Policy NI (2014):** The Northern Ireland Public Procurement Policy document sets out the policies adopted by the NI Executive and the organisational structures that have been established to implement them, along with the twelve procurement principles which govern the administration of public procurement.

u) **Public Supply Contracts Regulations (1995):** Defines the purchase or hire of goods by public authorities.

v) **Regulatory Investigative Powers Act (2000):** Defines the need to monitor staff actions in terms of illegal abuse.

w) General Data Protection Regulation (EU 2016/679)

x) Data Protection Act (2018)
y) Network and Information Systems Directive (EU 2016/1148)
z) 283473/NHS Information Governance: Guidance on Legal and Professional Obligations, Sept 2007
aa) BS ISO/IEC 17799:2005; BS ISO/IEC 27001:2005 Information Security
bb) 280361/NHS Information Security Management: NHS Code of Practice,
Apr 2007
cc) ITIL Infrastructure Library: ITIL Best Practice for Security Management
dd) BS ISO/IEC 20000:1-2011IT Service Management
ee) BS 25999-1:2006; BS 25999-2:2007 Business Continuity Management
ff) NCSC UK Technical Authority for Information Assurance (www.ncsc.gov.uk)
gg) UK Resilience – Civil Contingencies Act 1994 (www.ukresilience.info/ccact/index.shtm)
hh) BHSCT General Procurement Guidance
ii) BHSCT Good Practice Printing Guidelines
jj) BHSCT System Management Charter
kk) BHSCT Intranet Site – IT & Telecommunications

BHSCT Intranet Site – Information Governance

8.0 APPENDICES

Appendix I Third Party Statement of Compliance
Appendix II Data Protection Principles
Appendix III Glossary of Terms

9.0 NURSING AND MIDWIFERY STUDENTS

Nursing and/or Midwifery students on pre-registration education programmes, approved under relevant 2018/2019 NMC education standards, must be given the opportunity to have experience of and become proficient in **the ICT security policy** where required by the student's programme. This experience must be under the appropriate supervision of a registered nurse, registered midwife or registered health and social care professional who is adequately experienced in this skill and who will be accountable for determining the required level of direct or indirect supervision and responsible for signing/countersigning documentation.

Direct and indirect supervision

- Direct supervision means that the supervising registered nurse, registered midwife or registered health and social care professional is actually present and works alongside the student when they are undertaking a delegated role or activity.
- Indirect supervision occurs when the registered nurse, registered midwife or registered health and social care professional does not

directly observe the student undertaking a delegated role or activity. (NIPEC, 2020)

This policy has been developed in accordance with the above statement.

Wording within this section must not be removed.

10.0 EQUALITY IMPACT ASSESSMENT

The Trust has legal responsibilities in terms of equality (Section 75 of the Northern Ireland Act 1998), disability discrimination and human rights to undertake a screening exercise to ascertain if the policy has potential impact and if it must be subject to a full impact assessment. The process is the responsibility of the Policy Author. The template to be complete by the Policy Author and guidance are available on the Trust Intranet or via this **link**.

All policies (apart from those regionally adopted) must complete the template and submit with a copy of the policy to the Equality & Planning Team via the generic email address equalityscreenings@belfasttrust.hscni.net

The outcome of the equality screening for the policy is:

Major impact ☐
Minor impact ☐
No impact ☐

Wording within this section must not be removed

11.0 DATA PROTECTION IMPACT ASSESSMENT

New activities involving collecting and using personal data can result in privacy risks. In line with requirements of the General Data Protection Regulation and the Data Protection Act 2018 the Trust considers the impact on the privacy of individuals and ways to militate against any risks. A screening exercise must be carried out by the Policy Author to ascertain if the policy must be subject to a full assessment. Guidance is available on the Trust Intranet or via this **link**.

If a full impact assessment is required, the Policy Author must carry out the process. They can contact colleagues in the Information Governance Department for advice on Tel: 028 950 46576

Completed Data Protection Impact Assessment forms must be returned to the Equality & Planning Team via the generic email address equalityscreenings@belfasttrust.hscni.net

The outcome of the Data Protection Impact Assessment screening for the policy is:

Not necessary – no personal data involved ☐
A full data protection impact assessment is required ☐
A full data protection impact assessment is not required ☐

Wording within this section must not be removed.

12.0 RURAL NEEDS IMPACT ASSESSMENT

The Trust has a legal responsibility to have due regard to rural needs when developing, adopting, implementing or revising policies, and when designing and delivering public services. A screening exercise should be carried out by the Policy Author to ascertain if the policy must be subject to a full assessment. Guidance is available on the Trust Intranet or via this link.

If a full assessment is required the Policy Author must complete the shortened rural needs assessment template on the Trust Intranet. Each Directorate has a Rural Needs Champion who can provide support/assistance.

Completed Rural Impact Assessment forms must be returned to the Equality & Planning Team via the generic email address equalityscreenings@belfasttrust.hscni.net

Wording within this section must not be removed.

13.0 REASONABLE ADJUSTMENT ASSESSMENT

Under the Disability Discrimination Act 1995 (as amended) (DDA), all staff/ service providers have a duty to make Reasonable Adjustments to any barrier a person with a disability faces when accessing or using goods, facilities and services, in order to remove or reduce such barriers. E.g. physical access, communicating with people who have a disability, producing information such as leaflets or letters in accessible alternative formats. E.g. easy read, braille, or audio or being flexible regarding appointments. This is a non-delegable duty.

The policy has been developed in accordance with the Trust's legal duty to consider the need to make reasonable adjustments under the DDA.

Wording within this section must not be removed.

SIGNATORIES

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

01/04/2021

_____ Date: _____

Name: Charlene Stoops
Title: Director of Performance, Planning & Informatics

01/04/2021

_____ Date: _____

Name: Dr Cathy Jack
Title: Chief Executive

Appendix I – Third Party Statement of Compliance

This Statement of Compliance is a minimum requirement, and for particular organisations or applications/systems, may be supplemented by additional requirements identified by BHSCT.

I .....of .....
(name of CEO or equivalent) (name of organisation)
certify that the following security measures are in place and will be adhered to.

Information Security Management

1. Responsibility for Information Security has been assigned to an appropriate member, or members, of staff.
2. There is an Information Security Policy that addresses the overall requirements of information security.
3. All contracts (staff, contractor and third party) contain clauses that clearly identify information security & data protection responsibilities.
4. All staff members are provided with appropriate training on information security & data protection requirements.

Confidentiality and Data Protection.

1. The organisation's design, operation, use and management of BHSCT information systems comply with current relevant criminal and civil law and statutory, regulatory and contractual obligations
2. All BHSCT person identifiable data processed outside the UK complies with the General Data Protection Regulation (EU 2016/679) and Data Protection Act (2018) and Department of Health (NI) guidelines.
3. BHSCT information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of BHSCT information are appropriately respected.
4. The organisation abides by the BHSCT ICT Security Policy and associated documentation.
5. There are appropriate measures to control access to BHSCT information for both staff within the organisation's employ and other external individuals and 3rd party organisations who may be granted access to the organisation's ICT infrastructure.
6. There are appropriate confidentiality audit procedures in place to monitor access to BHSCT information & systems.
7. All transfers of personal and sensitive information are conducted in a secure and confidential manner.

Information Security

8. Policy and procedures are in place to ensure that Information & Communication Technology (ICT) networks operate securely.
9. Policies and procedures are in place to ensure that mobile computing and teleworking are secure.
10. Unauthorised access to premises, equipment, records and other assets is prevented.

11. Documented plans and procedures are in place to support business continuity in the event of power failures, system failures, natural disasters and other disruptions.
12. Documented incident management and reporting procedures are in place, including formal notification to BHSCT of incidents which directly or indirectly may have an impact on BHSCT information or systems.

Audit / Inspection

13. The organisation will facilitate audit or inspection by BHSCT authorised personnel as required to provide assurances that configuration/protection of systems/information is in accordance with this statement of compliance.
14. Any significant changes in status of the organisation will be communicated to the BHSCT Senior Information Risk Owner (S.I.R.O).

Signature

I certify that the above is true and understand that continuing failure to meet some or all parts of this Statement of Compliance may result in disconnection from BHSCT network and further action if appropriate.

Signature:..... **Date**.....
The signatory must carry the specific authority of the Chief Executive or equivalent

Signature:..... **Date**.....
This must be countersigned by the nominated individual responsible for ICT/Information Security.

Appendix III - Data Protection Principles

Users have a responsibility to process and store data in a manner that complies with the General Data Protection Regulation (EU 2016/679), Data Protection Act (2018), Network and Information Systems Regulations (2018) and any other relevant legislation. The General Data Protection Regulation (GDPR) lays down clear principles for the processing of data. These principles are summarised below. Users should also refer to the Trusts Data Protection and Protection of Personal Information Policy (TP026/08); this section merely outlines the principles of Data Protection.

If you have any queries or concerns about compliance with the GDPR 2018, registration or any other Data Protection guidance issues, please contact the Trusts Data Protection Office.

Article 5 - The Six Principles of the GDPR 2018

Article 5 of the GDPR requires that personal data shall be:
a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Appendix IV - Glossary of Terms

BHSCT	Belfast Health and Social Care Trust
BHSCT Senior Manager	Any Senior Manager within BHSCT at Tier 4 level or above
Business Continuity	Business continuity is the set of activities BHSCT will carry out in order to ensure that critical business services will remain available.
Data Protection Act (2018)	DPA2018 is an UK Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation (GDPR)
Disaster Recovery	Disaster recovery is the process or plan by which BHSCT can recover systems or infrastructure following a disaster.
End of Life	End of Life refers to when either the manufacturer / supplier can no longer support the software/system itself or the underlying infrastructure (e.g. desktop operating system), or is no longer supported by the Trust and or its suppliers.
FOI/FOIA	Freedom of Information / Freedom of Information Act. This is an Act that obliges the public sector generally to make open information about their activities, services and methods of service. The information can be stored in any format – paper or electronic.
GDPR	General Data Protection Regulation (EU) 2016/679 This is an EU regulation, which came into force on 25 May 2018. This regulation intends to strengthen and unify data protection for all individuals within the European Union (EU).
[redacted]	[redacted]
IAO	Information Asset Owner provides assurance to SIRO that information risk is being managed effectively in respect of the information assets that they 'own'.
ICT	Information and Communication Technologies. This includes physical devices such as computers, servers, laptops, thin clients, tablets, phones, smartphones, removable media, printers, scanners, pagers. It also includes communication technologies including telecomms and paging, networking, server and storage infrastructures.
ICT Service Desk	For the purpose of this policy this is the primary point of contact for all users who seek assistance or advice on the use of Trust ICT.
Information	For the purpose of this policy *information* includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on disk, tape and other electronic media or spoken in conversation or over the telephone.
Information System	For the purpose of this policy *Information System* is defined to be any computerised system that holds information related to

	the business of the Trust. This may range from a freestanding PC system up to a wide area network (WAN).
NIS	Network and Information Systems Regulations (2018) This Regulation was transposed from the NIS Directive (EU 2016/1148) into UK Law on 25 May 2018, aimed at improving the overall level of cybersecurity nationally. This regulation focuses on the availability of crucial network and information systems in order to protect the UK's critical infrastructure and thereby ensure service continuity.
Security	Security means the prevention of loss or corruption, and this Policy's objective is to preserve: - **Confidentiality** Data access is confined to those with specific authority to view the data. **Integrity** Information must be accurate, reliable and complete. This also implies the need to examine inputting processes and the specification of appropriate procedures. **Availability** Data output must be delivered to the point where it is needed, when it is needed.
SIRO	Senior Information Risk Owner is responsible for ensuring a culture of information risk management is in place across BHSCT.
User	Any person who uses/accesses Trust ICT Equipment / Systems / Information