NHS
Stockport
NHS Foundation Trust

INFORMATION SECURITY POLICY

CONTENTS AND PAGE NUMBER

EXECUTIVE SUMMARY

The purpose of this information security policy is to protect, to a consistently high standard, all information assets within Stockport NHS Foundation Trust, including patient records, staff records and other corporate information, from potentially damaging threats, whether internal or external, deliberate or accidental.

Information within Stockport NHS Trust Foundation Trust exists in many forms and this policy includes the protection of data stored electronically, transmitted across networks and printed or written on paper to safeguard the information of Stockport NHS Foundation Trust.

Stockport NHS Foundation Trust has a legal obligation to comply with all appropriate legislation in respect of Data Protection and Information Security

The Data Protection Act 2018 and the UK General Data Protection Regulation (UKGDPR) regulates the processing of personal data held in manual or electronic form.

The Act requires that "Personal data shall be 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"

The Computer Misuse Act 1990 made provision for securing computer material against unauthorised access or modification by making a criminal offence to gain unauthorised access or modify computer material or to do so with intent to commit or facilitate further an offences (by hacking) .

The Information Commissioner can impose financial penalties of £17.5 million or up to 4% of annual global turnover, whichever is higher, against organisations for serious breaches of the data protection act and GDPR. There are also criminal prosecution and custodial sentences against individuals who knowingly, recklessly or deliberately misuse personal data (under Section 170 of the Data Protection Act 2018).

Director of Informatics

SCOPE AND PURPOSE

This policy applies to Stockport NHS Foundation Trust, referred to as the 'Trust', and includes all hospitals, units and community health services managed by Stockport NHS Foundation Trust.

The objective of information security is to ensure business continuity and minimise damage by preventing and reducing the likelihood and impact of any information security incidents.

The aim of the information security policy is to preserve confidentiality, integrity and availability of data.

The implementation of this policy is mandatory to maintain and demonstrate Stockport NHS Foundation Trust's commitment to information security and the protection of all its information assets.

This policy covers all information systems purchased, developed and managed by, or on behalf of, the Trust.

The scope of the Trusts Information Security Management System (ISMS) is currently in relation to the provision of the Trusts local email service for the purpose of accrediting its email system to the DCB 1596 Secure Email Standard as required by NHS Digital.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate.

This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

ROLES AND RESPONSIBILITIES

Senior Information Risk Owner (SIRO):

The Chief Finance Officer is the designated SIRO and has overall responsibility for maintaining this policy and providing guidance on its implementation. The SIRO takes ownership of the risk management of information assets and assures risk assessment processes to the Board.

Information Asset Owners (IAO's):

IAO's are operationally responsible at senior levels for all information assets within their division areas. IAO's should understand and address the levels of risk in relation to the business assets they own and provide assurance to the SIRO on the security and use of those assets on quarterly and annual basis of review.

Information Asset Administrators (IAA's):

IAA's work at local divisions/departmental level and ensure that policies and procedures are in place for all information assets and that these are followed, recognise and report actual and potential security incidents, liaise with the IAO on incident management and ensure information asset registers are accurate and up to date.

The IAA should complete a 'Data Protection Impact Assessment' (DPIA), for each information asset and ensure that the DPIA is reviewed on an annual basis. The DPIA documentation can be found on the IG & Security Microsite or by contacting the Information Governance team.
The IAA is responsible for carrying out audits of who has accessed or attempted to access confidential information in line with section 8 of this policy.

Caldicott Guardian:

The Caldecott Guardian is the Trust's Medical Director and is responsible for safeguarding the confidentiality of patient and service-user information and enabling appropriate information-sharing.

Information Governance and Security Group:

The Information Governance and Security Group is responsible for reviewing this policy and ensuring the effective implementation of this policy and for the management and security of information assets.

It a formal working group to oversee and coordinate the technical and organisational security measures that need to be place to for all the key Information assets to ensure the confidentiality, integrity and availability of information and comply with the ISO 27001 Information Security Standard.

Information Security Assurance is key requirement of the Data Security and Protection Toolkit. Membership of the Information Governance and Security Group includes system managers / information asset administrators (IAAs) to represent the Trust key information systems.

Digital Technology Support :

The Digital Technology Support department is responsible for maintaining the hardware and software components of the IT and communications Infrastructure and, implementing all necessary technical and physical security controls to mitigate information security and cyber security risks.

All Trust Managers:

All managers are directly responsible for implementing the policies and procedures within their division areas.

All Trust Staff:

It is the responsibility of each employee to adhere to the policies and procedures and undertake data security awareness training.

GLOSSARY OF TERMS

Information Asset

Information assets are definable information resources owned or contracted by an organisation that are valuable' to the business of the organisation.

ISMS – Information Security Management System:

An information security management system (ISMS) is a set of policies and procedures concerned with information security management to minimise the risk to data and ensure business continuity. The Trust's ISMS document is part of its compliance with the ISO/IEC 27001 Information Security Standard and is available to view on the Trust's IG & Security Microsite.

Confidentiality

Ensuring that personal, sensitive and/or business critical information is appropriately protected from unauthorised access and can only be accessed by those with an approved need to access that information

Integrity

Ensuring that information has not been corrupted, falsely altered or otherwise changed such that it can no longer be relied upon

Availability

Ensuring that information is available at point of need to those authorised to access that information.

THE PROCESS

It is the policy of Stockport NHS Foundation Trust to ensure:

- Information is protected against unauthorised access.
- The confidentiality of information is assured
- Information is not disclosed to unauthorised persons through deliberate or careless actions
- The integrity of information is maintained
- The availability of information to authorised users when needed
- Regulatory and legislative requirements are met
- Business continuity plans exist, are maintained and regularly tested
- Data security awareness training is provided to all staff
- All breaches of information security, actual and suspected are recorded, reported and investigated
- A comprehensive Information Security Management System (ISMS) is established and maintained and is compliant with best practice as identified in ISO/IEC 27001:2013 international security management standard.
- An annual risk assessment is undertaken for all key information assets.
- Lessons are learnt from information security incidents, continual improvements to the ISMS identified and acted upon.

- Annual reporting of attainment is provided to the Department of Health through the NHS Data Security and Protection Toolkit.

- Standards, policies, security operating procedures and guidelines will be produced to support this policy and will include: virus control, access control, physical/environmental security, personnel security, acceptable use of e-mail and the Internet.

- A Data Protection Impact Assessment (DPIA) is completed for each Information Asset and any new / or change in service or system (information asset) which pertains to utilise person identifiable information

- Regular monitoring takes place relating to access to confidential information

The DPIA is a comprehensive document used to help ensure that the above information security requirements are appropriately addressed for each information asset, service or process.

The development, implementation and on-going management of a DPIA will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

An effective DPIA will therefore contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

In the context of this document “System” relates to the complete data handling solution (electronic or otherwise) of person identifiable / sensitive data.

In addition - NHS organisations are required to comply with the range of best security management practices as set out in ISO/IEC 27001:2013. The DPIA is a core component of an accreditation documentation set for those organisations that undertake formal accreditation processes for their information assets.

Where the system is available to multiple organisations, the DPIA must establish the necessary common policy, security parameters and operational framework for that system’s expected operation including any functional limitations or data constraints applicable to one or more bodies.

ISMS Objectives and Metrics:

The security objectives and metrics are detailed in the ISMS which is reviewed and accepted by the Information Governance and Security Group.

TRAINING

Induction:

All new staff must attend the Corporate Welcome session followed by local induction procedures which will provide information on how to access the mandatory data security awareness training.

Mandatory Training (e-learning):

All staff must complete their data security awareness mandatory training every year via the Trust's on-line ESR e-learning package. All new staff undertake data security awareness training provided at the corporate welcome session.

Staff who for whatever reason cannot undertake the on-line training module, may access trainer-led training as published in the Trust's Intranet and weekly communications update or complete a manual data security awareness workbook to be returned to to the IG team for marking and their training record updated on ESR.

Information Asset Owners/Administrators are required to undertake further Information Risk Management training

MONITORING COMPLIANCE

The Trust is committed to ensuring compliance with documents and will actively monitor the effectiveness of such documents.

Process for monitoring compliance with this policy

CQC Regulated Activities	Process for monitoring e.g. audit	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/group/ committee for review of results	Responsible individual/group/ committee for development of action plan	Responsible individual/group/ committee for monitoring action plan and implementation
	Internal Audit Data Security and Protection Toolkit. External	Information Governance & Security Group	Annually	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group

CQC Regulated Activities	Process for monitoring e.g. audit	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/group/ committee for review of results	Responsible individual/group/ committee for development of action plan	Responsible individual/group/ committee for monitoring action plan and implementation
	Audit of ISO27001 accreditation					

DOCUMENT LAUNCH AND DISSEMINATION

Launch

The responsibility of implementing this policy, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff including agency staff to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

This document has been compiled by the Information Governance Team in consultation with Governance Leads for each Division by means of the Information Governance and Security Group.

This policy will be reviewed regularly to ensure it remains appropriate for Stockport NHS Foundation Trust and its ability to serve the community and its patients.

This policy is directly referenced to BS 1008 and any changes to policy need to be checked for compliance.

Dissemination

Once finalised, the document will be presented to the Information Governance and Security Group for approval and then to the Digital Informatics Group for validation. The document will then be displayed on the Information Governance & Security microsite on the Trust's intranet and on the Trust's website. Managers and Governance leads should ensure the information is cascaded to all staff.

REFERENCES AND ASSOCIATED DOCUMENTATION

- Information Governance Policy
- Information Governance and Security Incident Reporting and Management SOP
- IT Acceptable Use Policy
- Mobile Devices & Removable Media Security Policy
- Agile and Home Working Policy
- Photography/Video & Audio Records of Patients Policy
- Network Security Policy
- Data Protection & Confidentiality Policy
- Access to Personal Information (Subject Access) Policy
- Data Quality Policy
- Freedom of Information Policy
- Information Sharing and Transfer or Records Policy
- Information Lifecycle and Records Management Policy
- Disciplinary Policy
- Incident Reporting SOP
- Data Protection Impact Assessment Proforma
- Risk Management Policy
- Registration Authority Policy
- Information Asset Management Policy
- BS 10008 – Evidential weight and legal admissibility of electronic information
- Information Security Management Systems (ISMS) document

EQUALITY IMPACT ASSESSMENT

Office Use Only

Submission Date:	*24/04/24*
Approved By:	*IGSG*
Full EIA needed:	No

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the**	INFORMATION SECURITY POLICY

	Policy/SOP/Service		
2	**Department/Divisions**	Information Governance & Security Dept	
3	**Details of the Person responsible for the EIA**	**Name:** **Job Title:** **Contact Details:**	Joan Carr I.G. Co-ordinator 0161 419 4364
4	**What are the main aims and objectives of the Policy/SOP/Service?**	This policy has been developed to protect the organisation from hazards and threats, to ensure that the valuable information held in information systems is secure from accidental or deliberate unauthorised modification or disclosure.	

For the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a <u>differential</u> impact on any of the protected characteristics below? Please state whether it is positive or negative. What data do you have to evidence this?** **Consider:** • What does existing evidence show? E.g. consultations, demographic data, questionnaires, equality monitoring data, analysis of complaints. • Are all people from the protected characteristics equally accessing the service?	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Produce action plan if further data/evidence needed ✓ Re-visit after the designated time period to check for improvement.	**Lead**
Age	Workforce Data: Average age 44.5 It is unlikely to affect people of a particular age disproportionately.	No differential impact See general comments	
Carers	Trust Workforce: No Data It is unlikely to affect carers disproportionately	No differential impact See general comments	
Disability	Trust Workforce: 3.32% report disability. 11.94% not declared It is unlikely to affect people with a disability disproportionately	No differential impact See general comments	

Race / Ethnicity	Trust Workforce: BAME make up 16.18% It is unlikely to affect people of a particular gender disproportionately.	No differential impact See general comments	
Gender	Trust Workforce: 79.9% female It is unlikely to affect people who have gender reassignment disproportionately.	No differential impact See general comments	
Gender Reassignment	Trust Workforce: No Data It is unlikely to affect people of a particular marital status disproportionately	No differential impact See general comments	
Marriage & Civil Partnership	Trust Workforce: 54.9% married & 0.7% Civil Partnership It is unlikely to affect a pregnant woman disproportionately.	No differential impact See general comments	
Pregnancy & Maternity	Trust Workforce: 2.14% on maternity or adoption leave* It is unlikely to affect people of any particular religion or belief disproportionately.	No differential impact See general comments	
Religion & Belief	Trust Workforce: 52.47% Christian It is unlikely to affect people of any particular religion or belief disproportionately.	No differential impact See general comments	
Sexual Orientation	Trust Workforce: 2.12% LGBT 20.09% did not want to declare It is unlikely to affect people of any particular sexual orientation disproportionately	No differential impact See general comments	
General Comments across all equality strands	The policy relates to the Trusts requirements to maintain information governance for all subjects (Patients and Staff) and does not concern itself with specifics	Adjustments are made to computer equipment, furniture or software to ensure that all workers have equal access to computers, training and compliant with health and safety standards.	

Action Plan

What actions have been identified to ensure equal access and fairness for all .

Action	Lead	Timescales	Review &Comments

EIA Sign-Off	**Your completed EIA should be sent to Equality, Diversity & Inclusion Manager for approval:** equality@stockport.nhs.uk **0161 419 4784**

Quality

(Clinical and Quality Impact Assessment, Please record 'No Impact' if this is the case)

Date of Initial Review	18/04/2022
Date of Last Review	18/04/2022

Area of Impact		Consequence	Likelihood	Total	Potential Impact	Impact (Positive or Negative)	Action	Owner
Quality	Duty of Quality			0	How does it impact adversely the rights and pledges of the NHS Constitution?	No Impact		
					How does the impact affect the organisation's commitment to being an employer of choice?	No Impact		
					What is the equality impact on race, gender, age, disability, sexual orientation, religion and belief, gender reassignment, pregnancy and maternity for individuals' access to services and experience of the service?	No Impact		
	Patient Safety			0	How will this impact on the organisation's duty to protect children, young people, and adults?	No Impact		
					How will it impact on patient safety? • Infection rates • Medication errors • Significant untoward incidents and serious adverse events • Mortality & Morbidity • Failure to recognise a deteriorating patient • Safe staffing levels	No Impact		
					How will it impact on preventable harm? (eg. slips, trips, falls)?	No Impact		
					How will it impact upon the reliability of safety systems? (eg. WHO checklist)	No Impact		

					How will it impact on systems and processes for ensuring that the risk of healthcare acquired infections is reduced?	No Impact		
					How will this impact on workforce capability, care and/or skills?	No Impact		
Experience	**Patient Experience**			**0**	What impact is it likely to have on self-reported experience of patients and service users? (Response to national / local surveys / complaints / PALS/incidents)	No Impact		
					How will it impact on choice?	No Impact		
					Will there be an impact on waiting times?	No Impact		
					How will it impact upon the compassionate and personalised care agenda?	No Impact		
	Staff Experience			**0**	How will it impact on recruitment of staff?	No Impact		
					What will the impact be on staff turnover and absentee rates?	No Impact		
					How will it impact on staff satisfaction surveys?	No Impact		
Effectiveness	**Clinical Effectiveness and Outcomes**			**0**	How does it impact on implementation of evidence-based practice?	No Impact		
					How will it impact on patient's length of stay?	No Impact		
					Will it reduce/impact on variations in care? (eg. readmission rates)	No Impact		
					What will the impact be upon clinical and cost-effective care delivery?	No Impact		
					How does it impact upon care pathway(s)? eg. Mortality	No Impact		
					How will it impact on target performance?	No Impact		
Other	**Please use this section to detail any other impacts to clinical and quality that are not listed in the questions.**							

Data Protection Impact Assessment

The Trust will have to ensure that any third parties used to process or share personal data with will need to ensure the data is secure and confidential and, a data processing agreement or information sharing agreement may need to be in place.

To assess the implications of using personal data, a risk assessment called a Data Protection Impact Assessment (DPIA) is required to

ensure the Trust is complying with its legal obligations under the Data Protection Act 2018 and UK GDPR.

If you are doing any of the following you will need to complete a DPIA:

- Setting up a new process using personal confidential data (PCD)
- Changing an existing process which changes the way personal confidential data is used
- Procuring a new information system which holds personal confidential data

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

The DPIA Process:

1) Complete the screening questions below – this is to determine whether or not completion of a full DPIA is required.
2) If a full DPIA is required, you will be advised by the Information Governance Team and sent the full DPIA proforma for completion.

If DPIA's are not completed, there may be data protection concerns that have not been identified which could result in breaching the Data Protection Act / UK GDPR.

Advice/Guidance on completing the screening questions or the full DPIA can be provided by the Information Governance Team by contacting information.governance@stockport.nhs.uk

DPIA Screening Questions

		Yes	No	Unsure	Comments *Document initial comments on the issue and the privacy impacts or clarification on why it is not an issue*
A)	Will the process described involve the collection of new information about individuals?		x		
B)	Does the information you are intending to process identify individuals (e.g. demographic information such as name, address, DOB, telephone, NHS number)?		x		
C)	Does the information you are intending toprocess involve sensitive information e.g.health records, criminal records or other information people would consider particularly private or raise privacy concerns?		x		
D)	Are you using information about individuals for a purpose it is not currentlyused for, or in a way it is not currently used?		x		
E)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		x		

F)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		x		
G)	Does the initiative involve you using new technology which might be perceived asbeing intrusive? e.g. biometrics or facial recognition		x		
H)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		x		
I)	Will the initiative compel individuals to provide information about themselves?		x		

1. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

If you answered YES or UNSURE to any of the above, you need to continue with the Privacy Impact Assessment. Giving false information to any of the above that subsequently results in a yes response that you knowingly entered as a NO may result in an investigation being warranted which may invoke disciplinary procedures.

DOCUMENT INFORMATION

Type of Document	Policy
Title	Information Security Policy
Version Number	V9.1
Consultation	IG & Security Group Digital Informatics Group
Recommended By:	IG & Security Group
Approved By:	IG & Security Group Digital Informatics Group
Approval Date	24th April 2024

Next Review Date	April 2025
Document Author	Head of Information Governance & Security/DPO
Document Director	Director of Informatics
For use by:	All Trust employees
Specialty / Ward / Department (if local procedure document)	

Version	Date of change	Date of release	Changed by	Reason for change
9.1	Apr 24	Apr 24	Information Governance Coordinator	Annual review & EIA
9.0	Apr 23	Apr 23	Information Governance Coordinator	Changes to SIRO job title. Reference to data security awareness training delivered at Corporate Welcome for new staff and via trainer sessions onsite as well as manual workbooks
8.0	Apr 2022	Apr 2022	Information Governance Coordinator	Change of titles. Updated to remove and replace the reference to SLSP with DPIA
7.2	Mar 2021	Mar 2021	Information Governance Coordinator	Review and Siro title updated
7.1	Mar 2020	Mar 2020	Information Governance Coordinator	New Trust format and minor update to replace reference to IG Toolkit to DSP Toolkit and IG training to Data Security Awareness Training
5.3	Oct 2018	Oct 2018	Information Governance Coordinator	Updated legislation DPA 2018 references
5.2	Jan 2018	Jan 2018	Information Governance Coordinator	Included reference to GDPR
5.1	September 2017	September 2017	Information Governance Coordinator	Included references to Scope and Objectives of the ISMS
5.0	June 2016	June 2016	Information Governance Coordinator	Refresh
4.0	June 2014	June 2014	Information Governance	Additions to Introduction about relevant legislation and

			Coordinator	consequences. Change of SIRO. Removed appendices (SLSP) as separate SOP
3.0	February 2013	February 2013	Information Governance Coordinator	Added requirement to complete PIAs. Changes to System Level Security Procedure.
2.1	September 2011	September 2011	Information Governance Coordinator	Section 2 - Inclusion of first paragraph for clarification around the scope of the document. Other minor amendments to wording.
2.0 (Final)	March 2011	March 2011	Information Governance Coordinator	Included Audit Trail monitoring form as an appendix of the System Level Security Procedure Template.
2.0 (Final)	March 2011	March 2011	Information Governance Coordinator	Included additional 'Best Practice' guidelines in System Level Security Procedure Template (blue text).
2.0 (Final)	March 2011	March 2011	Information Governance Coordinator	Included Contact Number of Risk and Safety Team.
2.0 (Draft)	January 2011	January 2011	Information Governance Coordinator	Adopted the new Trust Policy format. Significant Changes Made. Including inclusion of roles & responsibilities; definitions; implementation and monitoring arrangements and; SLSP template in the appendix.
1.0	May 2007	May 2007	Assistant Director Information Governance & Security	New Policy