INFORMATION GOVERNANCE

POLICY

CONTENTS

EXECUTIVE SUMMARY 4
SCOPE AND PURPOSE 4
ROLES AND RESPONSIBILITIES 6
Data Quality Assurance Group 6
Digital and Informatics Group 6
The Board of Directors 6
Senior Information Risk Owner (SIRO) 7
Caldicott Guardian 7
Information Governance Team and Data Protection Officer 7
Director of Informatics 7
All Trust Managers: 7
All Trust Staff 8
GLOSSARY OF TERMS 8
Person Identifiable Information 8
Sensitive and Special Category Information 8
THE PROCESS 9
Data Protection, Confidentiality, and Privacy 9
Information Security and Cyber Security 9
Data Quality Assurance 10
Records Management 10
Freedom of Information 10
Subject Access 11
TRAINING 11
Induction 11
Mandatory Training (e-learning) 11
Specialist Roles: 12
Specialist roles include: 12
Additional / Ad hoc Training: 12
MONITORING COMPLIANCE 12
Monitoring 13
Data Security and protection Toolkit Assessment: 13
Incident Reporting & Management 14
DOCUMENT LAUNCH AND DISSEMINATION 15
Launch 15
Dissemination 15

REFERENCES AND ASSOCIATED DOCUMENTATION 15
Direct links 15
Data Protection Act 2018 15
The UK General Data Protection Regulation 15
The Records Management Code of Practice 2023 15
BS ISO/IEC 27001:2013 Standard for Information Security Management 15
DCB1596: Secure Email 15
Health and Social Care Act 2012 15
Counter-Terrorism and Security Act 2015 16
National Data Guardian for Health and Care 2017 report: Impact and influence for patients and service users 16
A Manual for Caldicott Guardians 2017 16
Data Security and Protection Toolkit 16
EQUALITY IMPACT ASSESSMENT 16
Action Plan 18
Quality 19
Data Protection Impact Assessment 20
DPIA Screening Questions 20
DOCUMENT INFORMATION 21
APPENDICES 23
Appendix (A1): Information Governance Management Framework 23
Appendix (A2): Trust Assurance Framework 24
Appendix (B): Information Governance (Training Needs Analysis) 24
Appendix (C): Guidance on Legal and Professional Obligation 26

EXECUTIVE SUMMARY

This document and associated policies and procedures identify the principles required to ensure that all staff comply with the law and best practice when handling information. This document should be read alongside the Trust's associated policies.
Information Governance is to do with the rules and regulations that should be followed when we process information. It allows organisations and individuals to ensure information is processed **legally, securely, efficiently and effectively.**

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently and securely managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

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.

This policy applies to all forms of information held by the Trust, including (but not limited to):

- Patient health records
- Human Resources Records
- Organisational and administrative Information, e.g. estates, corporate planning, supplies ordering, financial and accounting records.

This policy covers all aspects of handling information, including (but not limited to):

- Information recording or processing systems whether paper or electronic, X-Rays, photographic, slides, video, audio, outputs and images
- Transmission of information, such as fax, e-mail, text, post, telephone, video.
- Mobile devices and digital media (e.g. CD-ROM, DVDs, hard drives, removable memory, smartphones, tablets and compatible internal/external media

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

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.

The policy is set out to comply with (but not limited to) the following legislation and regulatory framework:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Health Service (Control of Patient Information) Regulations 2002
- The Common Law Duty of Confidentiality
- Human Rights Act 1998
- Freedom of Information Act 2000
- The Re-use of Public Sector Information Regulations 2005
- Environmental Information Regulations 2004
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- The Access to Medical Reports Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1990
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Public Interest Disclosure Act 1998
- The Public Records Act 1958
- Counter-Terrorism and Security Act 2015
- Administrative Law
- Health and Social Care Act 2012
- NHS Act 2006
- Road Traffics Act 1988
- Regulations under Health and Safety at Work Act 1974
- Human Fertilisation and Embryology Act 1990
- Abortions Regulations 1991
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000
- National Data Guardian for Health and Care 2017 report: Impact and influence for patients and service users
- A Manual for Caldicott Guardians 2017
- Confidentiality: NHS Code of Practice 2003
- The Records Management Code of Practice 2021
- Information Security Management: NHS Code of Practice 2007
- BS ISO/IEC 270001:2013 Standard for Information Security Management
- Data Security and Protection Toolkit (DSPT)
- DCB1596 Secure Email Standard
- Information Asset Management Policy

Please refer to ***Appendix C*** for guidance on the legislation and regulatory framework. The guidance outlines the impact of these provisions on NHS Trusts and information and identifies the trusts responsibilities and approach to meet these requirements.

ROLES AND RESPONSIBILITIES

Information Governance & Security Group (IGSG)

The IGSG is the Trust forum with delegated authority to oversee Information Governance developments issues within the Trust. It reports to the Corporate Quality Board (for KPIs) and to the Digital and Informatics Group.

The Senior Information Risk Owner (SIRO) and Caldicott Guardian, whilst not members of the IGSG, are members of the Finance and Performance Group and have regular monthly meetings with the Head of Information Governance/DPO to discuss the key issues report from the documentation from IGSG meetings. Membership of the IGSG includes a representative from the clinical divisions and corporate divisional areas of the Trust.

It is the role of the IGSG to define the Trust's polices in respect of Information Governance, considering legislation, regulations, standards, and national NHS requirements.

The IGSG will oversee Information Governance issues including breaches of confidentiality and security, ensuring appropriate action is taken.

The IGSG will ensure that all areas of Information Governance are adequately represented by the appropriate subgroups to ensure effective delivery of the Data Security and Protection Toolkit (DSPT) requirements and compliance with associated standards and legislation.

Data Quality Assurance Group

Data Quality forms a key part of the clinical information assurance element of the DSPT. The Data Quality Assurance Group should oversee compliance with the clinical information assurance requirements, as well as the secondary use assurance elements of the toolkit.

The membership of the Data Quality Assurance Group includes adequate representation from the appropriate divisions, including information, outpatients, and the emergency department.

Digital and Informatics Group

The IGSG reports key issues to the Digital and Informatics Group and submits IG policies for formal validation, being a Board Assurance Committee.

The Board of Directors

The Chief Executive has overall responsibility for Information Governance, as the Accountable Officer for the Trust. The Board of Directors is responsible for ensuring that sufficient resources are provided to support the requirements of the policy and management framework.

Senior Information Risk Owner (SIRO)

The Chief Finance Officer, will act as the Trust's Senior Information Risk Owner and the Trust Board Champion for Information Governance, Data Quality and Records Management, including Freedom of Information.

The Chief Finance Officer is responsible for overseeing implementation and performance assessment of Information Governance.

Ultimate responsibility for Information Governance within the Trust lies with the Board of Directors. The Digital and Informatics Group has delegated responsibility from the Board of Directors for Information Governance.

Caldicott Guardian

The Caldicott Guardian is the Trust's Medical Director and has responsibility for safeguarding the confidentiality of patient information.

Information Governance Team and Data Protection Officer

The Information Governance Team is responsible for managing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance within the Trust and raising awareness of Information Governance through training, with key members attending the IGSG meetings.

The Data Protection Officer is responsible to ensuring compliance with data protection and associated legislation.

Director of Informatics

The Director of Informatics has overall management oversight of Information Governance.

All Trust Managers:

Managers within the Trust are responsible for ensuring that the policy, and other associated policies and supporting standards and guidelines are built into local processes and that there is on-going compliance.

Managers are accountable for the communication about and compliance with Trust policies, and must ensure that staff are adequately trained and apply the appropriate guidelines.

All Trust Staff

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day-to-day basis.

All staff is responsible for any records or data they create and what they do with information they use.

Staff must ensure they undertake annual data security awareness training to maintain their knowledge and skills according to Trust mandatory training requirements.

All staff has a responsibility to adhere to information governance standards and the data protection act which are written into the terms and conditions of their contracts of employment.

GLOSSARY OF TERMS

Person Identifiable Information

This is also referred to as, “personal / confidential information” and relates to information about a person which would enable that person’s identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Sensitive and Special Category Information

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community, so needs greater protection. Sensitive information is wider than, but includes, data defined as special category data under the **“**Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK-GDPR)**,** which includes data relating racial/ethnicity, religion, sexual orientation, biometric and health data. In addition financial and security information is also likely to be deemed “sensitive”.

Data Security and Protection Toolkit (DSPT)

The Data Security and Protection Toolkit is an online self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

THE PROCESS

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff, as well as certain commercial information where appropriate.

The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

The following sections cover key elements of the Information Governance Policy and Framework:

Data Protection, Confidentiality, and Privacy

- The Trust regards all person identifiable information relating to patients as confidential
- The Trust regards all person identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act, Common Law Confidentiality and Freedom of Information Act.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).
- The Trust will undertake Data Protection Impact Assessments (DPIAs) for new systems or processes or changes to existing systems or processes that use and process personal data.

Information Security and Cyber Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements, including independent security/penetration testing of its systems and network infrastructure.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training

- The Trust will undertake risk assessments to determine appropriate security controls are in place for existing and new information systems
- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security
- The Trust will ensure effective disaster recovery and business continuity plans of its Information systems
- The Trust will use the Information Security Management NHS Code of Practice and BS ISO/IEC 27001:2013 best practice standard to establish and maintain an Information Security Management System (ISMS) and its compliance and certification with ISO 27001.

Data Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance
- The Trust will undertake or commission annual assessments and audits of its information
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality through policies, procedures, user manuals and training
- The Trust will ensure the accuracy of all clinical coding data, and the effective management of Payment by Results (PbR)

Records Management

- The Trust will establish and maintain policies and procedures for the effective management of records
- The Trust will undertake or commission annual assessments and audits of its records management arrangements
- Managers are expected to ensure effective records management within their services areas
- The Trust will promote effective records management through policies, procedures/user manuals and training
- The Trust will use the ‘Records Management: NHS Code of Practice’ as its standard for records management and retention schedules.

Freedom of Information

- Non-exempt information on the Trust and its services should be available to the public through a variety of media, in line with the Trust’s code of openness and its publication scheme under the terms of the Freedom of Information Act
- The Trust will establish and maintain policies and procedures to ensure compliance with the Freedom of Information Act 2000.

- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for compliance.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Trust will have clear procedures and arrangements for handling queries from the public

Subject Access

- The Trust will have clear procedures and arrangements to comply with the right of access, under Data Protection Act 2018 and the UK General Data Protection Regulation

- Patients will be provided with information and guidance to enable ready access to information relating to their own health care, their options for treatment and their rights under the Act.

- Staff will be provided with information and guidance to enable ready access to information relating to their employment and their rights under the Act (subject to exemptions in accordance with the Act)

- The Trusts Access to Personal Information (Subject Access) policy provides guidance regarding any subject access requests from patients, staff and their representatives including other organisations such as the police.

TRAINING

The Trust has also included Data Security Awareness Training within its core 'Mandatory' training programme which is delivered electronically via the ESR eLearning. The Trust has adopted the Core Skills Framework suite of mandatory training which allows staff to transfer within organisations that have adopted this framework, without the need to repeat training.
The Trust IG Training Needs Analysis documentation (see Appendix b) details mandatory and additional training for all staff, and Managers should ensure that staff are aware of and adhere to the requirements.

Compliance with this requirement will also provide assurance that we meet our legal obligations under the Data Protection Act, by ensuring staff are appropriately trained.

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 information governance training.

Mandatory Training (e-learning)

All staff must complete their corporate mandatory Data Security Awareness training every year via the Trust's ESR e-learning package. This is to ensure that staff develop and improve their knowledge and skills in the IG work area, in order to support the provision of high-quality health & social care.

There is additional training which specified staff must undertake. This training is available by contacting the IG Department and the IG Training Needs Analysis at Appendix (b) provides more information and details which staff are required to undertake the additional training.

Please see the IG training needs analysis at appendix (b) for details on which modules are mandatory for specific staff groups.

Staff who for whatever reason, for example those with learning/language difficulties, cannot undertake the on-line training module, may access trainer-led training as published in the Trust's training brochure at the discretion of their line manager and in liaison with the IG Team.

As part of Data Security Awareness e-learning training, staff will be required to undertake and pass an assessment at the end of the training session in order receive a satisfactory completion certificate.

Specialist Roles:

In addition to the basic mandated modules for all Trust staff, staff members in specialist roles, as set out below, should undertake and pass the modules outlined at appendix (b) every three years.

Specialist roles include:

- The Caldicott Guardian
- The Senior Information Risk Owner (SIRO)
- Data Protection Officer (DPO)
- Information Asset Owners (IAO)
- Information Asset Administrators (IAA)
- Subject Access Handlers
- Information Governance & Security Group members and members of any sub-groups

Training for these Groups may be delivered via a paperwork-book/assessment or ESR/eLfH.

Additional / Ad hoc Training:

The Information Governance team are responsible for co-ordinating ongoing training and awareness for all staff within the Trust.

Subsequent training needs will be identified through the appraisal process and/or the incident management process and can be provided on an ad hoc basis on request.

MONITORING COMPLIANCE

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

Monitoring

The Trust will regularly monitor and audit its Information Governance practices for compliance with this policy.
The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the policy is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Information Governance & Security Group, Health Informatics Strategy Board, Digital and Informatics Group and the Audit Committee, as appropriate.

Data Security and protection Toolkit Assessment:

An assessment of compliance with the requirements of DSPT will be undertaken each year.

The DSPT sets out the 10 National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether meeting the assertions, will demonstrate that the Trust is working towards or meeting the NDG standards which are set out under the following categories:

1. Personal Confidential Data
2. Staff Responsibilities
3. Training
4. Managing Data Access
5. Process Reviews
6. Responding to Incidents
7. Continuity Planning
8. Unsupported Systems
9. IT Protection
10. Accountable Suppliers

The Trust must comply with all 38 assertions and 110 of 149 mandatory evidence items of the DSPT, which will be independently audited on an annual basis as part of the Trusts internal audit plan.

The DSPT is made available to NHS Digital, Department of Health and Social Care and the CQC. An overview of an organisations compliance with DSPT is made publicly available

The Information Governance & Security Group (IGSG) and relevant subgroups will review and assess the status of the DSPT compliance. Proposed actions and improvement plans will also be determined by the group.

Incident Reporting & Management

All incidents should be reported in line with the incident management procedures and to the Information Governance Team, where necessary, and investigated by the appropriate risk co-ordinator / governance lead.

Examples of an Information governance incident include, but are not limited to, the following:

- Loss of patient/confidential data on portable/removable media
- Patient/confidential information in unsecured location
- Sharing and disclosing of passwords (e.g. PAS)
- Unauthorised access of patient/confidential information
- Unauthorised disclosure of patient/confidential information

Incident reports extracted from the incident management system (Datix) will be reviewed by the appropriate group i.e. Information Governance & Security Group, Divisional Quality Boards, to identify whether any further action is required, in addition to any actions taken at the time of the incident or by the risk co-ordinator / governance lead.

Any Serious Incidents and data losses should be handled by the Trust SI procedure and managed in accordance with the Department of Health 'Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation'.

All serious Incidents that meet the criteria for reporting to the Information Commissioners Office (ICO) should be reported on the DSPT and will be made available to the ICO, NHS Digital/NHS England, Department of Health and Social Care.

Any concerns or for further advice in relation to information governance / data security should be raised with the Information Governance Team.

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 Protection and Security Toolkit External Audit	Information Governance & Security Group	Annually	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group

DOCUMENT LAUNCH AND DISSEMINATION

Launch

Trust Website:
Information Governance & Security Microsite

Dissemination

Trust Website:
Information Governance & Security Microsite

REFERENCES AND ASSOCIATED DOCUMENTATION

Direct links

The following legal, regulatory and professional obligations have direct links to the source documents. These provide the scope of the obligations to NHS Trusts and identify the Trusts responsibilities and approach to meet these requirements.
Please view the links below for further information.

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

The UK General Data Protection Regulation
https://ukgdpr.org

The Records Management Code of Practice 2023

https://transform.england.nhs.uk/information-governance/guidance/records-management-code/BS ISO/IEC 27001:2013 Standard for Information Security Management
https://www.iso.org/isoiec-27001-information-security.html

DCB1596: Secure Email
https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb1596-secure-email

https://digital.nhs.uk/services/nhsmail/the-secure-email-standard/secure-email-standard-dcb1596-guidance

Health and Social Care Act 2012
http://www.legislation.gov.uk/ukpga/2012/7/pdfs/ukpga_20120007_en.pdf

Counter-Terrorism and Security Act 2015
http://www.legislation.gov.uk/ukpga/2015/6/pdfs/ukpga_20150006_en.pdf

National Data Guardian for Health and Care 2017 report: Impact and influence for patients and service users
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668729/NDG_Progress_Report_FINAL_v1.1.pdf

A Manual for Caldicott Guardians 2017
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

Data Security and Protection Toolkit
https://www.dsptoolkit.nhs.uk/?AspxAutoDetectCookieSupport=1

EQUALITY IMPACT ASSESSMENT

Office Use Only

Submission Date:	12/12/2023
Approved By:	*N Baynham*
Full EIA needed:	No

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

1	**Name of the Policy/SOP/Service**	Information Governance Policy	
2	**Department/Division**	Information Governance – IM&T	
3	**Details of the Person responsible for the EIA**	**Name:**	Joan Carr
		Job Title:	I.G. Co-ordinator
		Contact Details:	Information.governance@stockport.nhs.uk
4	**What are the main aims and objectives of the Policy/SOP/Service?**	To provide guidance for staff in order to maintain and uphold the Trusts information governance requirements	

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 Stockport Population Data: Largest age band 40 – 49 Older people are more likely to experience serious complications from the virus	- Consider are there any age related impacts? - Is the proposal for all ages or particular age groups? - Mitigating any increased risks. - Dignity & Modesty	
Carers	The 2011 Census showed there are 31,982 unpaid carers in Stockport. 6,970 (22% of all carers) provide 50+ hours of care per week. Signpost for Carers estimate the total value of unpaid care in Stockport is £570 million a year. Trust Workforce: No Data Carers are more likely to come into contact with vulnerable patients	- Chaperones - Mitigating any increased risks. - Accessible Information	
Disability	The 2011 census indicates that 18.4% of Stockport residents are living with a limiting long-term illness Trust Workforce: 3.32% report disability. 11.94% not declared COVID impacts are higher among people with long-term conditions COVID impacts are higher among people with long-term conditions	- Accessible communication. - BSL interpreters - Mental capacity - Pictorial images - Hearing loops - learning difficulties - visually impaired - Mitigating any increased risks. - Dignity & Modesty	
Race / Ethnicity	Stockport's Black & Minority Ethnic (BME) population has risen from just 4.3% in 2001 to around 8% at the 2011 Census Trust Workforce: BAME make up 16.18% People from Black, Asian and Minority Ethnic (BAME) backgrounds are more likely to experience serious complications from the virus	- Interpreters - Mitigating any increased risks. - Dignity & Modesty	

Gender	Stockport's population is split almost equally by gender (51.1% female, 48.9% male), which mirrors the national trend. Trust Workforce: 79.9% female Although women were more likely to have a positive COVID test, men were more likely to die from the disease	- Dignity & Modesty - Mitigating any increased risks. -	
Gender Reassignment	It is estimated that 1% of the UK population is gender variant, based on referrals to and diagnoses of people at gender identity clinics. This would equate to 3,000 people in the borough Trust Workforce: No Data Increased risk of severe COVID-19 in people who are on antiretroviral treatment and are not immunosuppressed.	- Dignity & Modesty - Mitigating any increased risks. - Gender Dysphoria - Treating in accordance to preferred identity. - Pronouns	
Marriage & Civil Partnership	38% married 0.2% of people in the 2011 census were in a civil partnership – a figure which is consistent across Stockport, the North West and nationally. Trust Workforce: 54.9% married & 0.7% Civil Partnership	- Mitigating any increased risks.	
Pregnancy & Maternity	2% fertility rate On average there are over 3,300 births to Stockport resident mothers each year. Trust Workforce: 2.14% on maternity or adoption leave* Pregnant women are included in the list of 'high risk' groups.	- Mitigating any increased risks. - Dignity & Modesty	
Religion & Belief	The majority of Stockport residents are Christian (63.2% - down from 75% at the last census), which is 4% greater than the national average. Trust Workforce: 52.47% Christian	- Interpreters - Mitigating any increased risks. - Dignity & Modesty - Religious beliefs	
Sexual Orientation	It is estimated that 5-7% of the UK population is LGB, which would equate to 15-21,000 people in the borough. Trust Workforce: 2.12% LGBT 20.09% did not want to declare	- Gender Dysphoria - Utilising Pronouns	
General Comments across all equality strands	This section is useful to clarify mitigations that will be applicable across all groups e.g. dignity and modesty.		

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

Quality

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

Date of Initial Review	18/12/2021
Date of Last Review	18/12/2021

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		x		

	concerns?				
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 Governance Policy
Version Number	V9.2
Consultation	Digital and Informatics Group
Recommended by	IG & Security Group
Approved by	IG & Security Group
Approval Date	27th November 2024
Next Review Date	November 2025
Document Author	Head of Information Governance & Security and DPO
Document Director	Director of Information
For use by	All Trust employees

Specialty / Ward / Department (*if local procedure document*)	

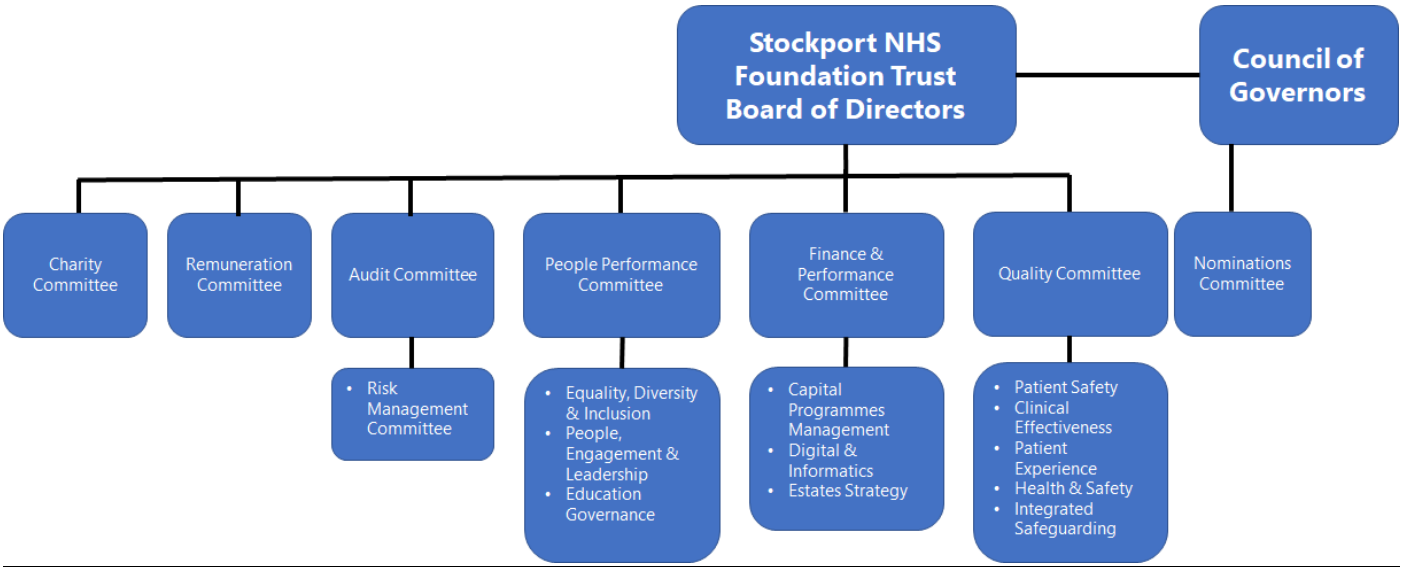
Version	Date of Change	Date of Release	Changed by	Reason for Change
9.2	Nov 2024	Nov 2024	IG	Review and specialist training
9.1	Dec 2023	Dec 2023	IG	Reworded the SIRO and Caldicott Guardian as members of F&P
9.0	Nov 2023	Nov 2023	IG	Added statement re police requests for patient/staff information and rewording of the IGSG section.
8.0	Nov 2022	Nov 2021	IG	Business Group changed to Division
7.3	Nov 2021	Nov 2021	IG	New template and further minor updates/additions to various sections, including control of patient information regulations, special category data, DPIAs, independent penetration testing, training.
7.2	Nov 2021	Nov 2021	IG	Updated Corporate Management and Trust Board Structure framework
7.1	Nov 2021	Nov 2021	IG	Update links and titles for GPDR, DQ Assurance Group and NHS Code of Practice
7.0	Jan 2021	Jan 2021	IG	Change of Title for SIRO, Executive statement and Caldicott Guardian
6.0	Feb 2020	Feb 2020	IG	Adopted the new Trust Policy Format.
5.4	Nov 2018	Nov 2018	IG	Multiple - Update of new Data Security and Protection Toolkit (replaced IG Toolkit)
5.3	Oct 2018	Oct 2018	IG	Multiple - Update of legislation. Updated the legislation and regulatory framework. Added Appendix C to provide the scope of the obligations to NHS Trusts and identifies the trusts responsibilities and approach to meet these requirements. Update of new Data Security and Protection Toolkit (replaced IG Toolkit)
5.2	Jan 2018	Jan 2018	IG	5 - Inclusion of reference to GDPR
5.1	September 2017	September 2017	IG	14 - Update to Assurance Structure following changes to business groups
5.0	April 2017	April 2017	IG	13 - Update to requirements for specialist training/TNA
4.1	July 2015	July 2015	IG	10 - Inclusion of separate subject access information
4.0	August 2014	August 2014	IG	Multiple 1, 13, 11 14 - Minor alterations/amendments to reporting Group information due to changes in framework Inclusion of reference to BS 10008 Amendment to IG Training procedures Updated Assurance Framework reporting structure
3.0	November 2013	November 2013	IG	6,7,8,10,12,14 - Minor alterations/additions to sentences in various sections including changes to committee structure. Also

				inclusion of the IG Refresher Module in the IG E-learning TNA.
2.3	November 2012	November 2012	IG	14 - Alterations to committee structure.
2.2	September 2011	September 2011	IG	11, 12 - Minor alterations to wording, Section 6.3.3 and Section 6.4
2.1	January 2011	January 2011	IG	5 - Section 2 - Inclusion of first paragraph for clarification around the scope of the document. Other minor amendments to wording.
2.0 (Final)	January 2011	January 2011	IG	No Changes
2.0 (Draft)	January 2011	January 2011	IG	Multiple - Adopted the new Trust Policy format. Significant Changes Made. Including inclusion of committee roles responsibilities; definitions; an incident reporting section; a structure diagram; training requirements and; implementation and monitoring arrangements.
1.0	May 2007	May 2007	Assistant Director of Information Governance and Security	New Policy

APPENDICES

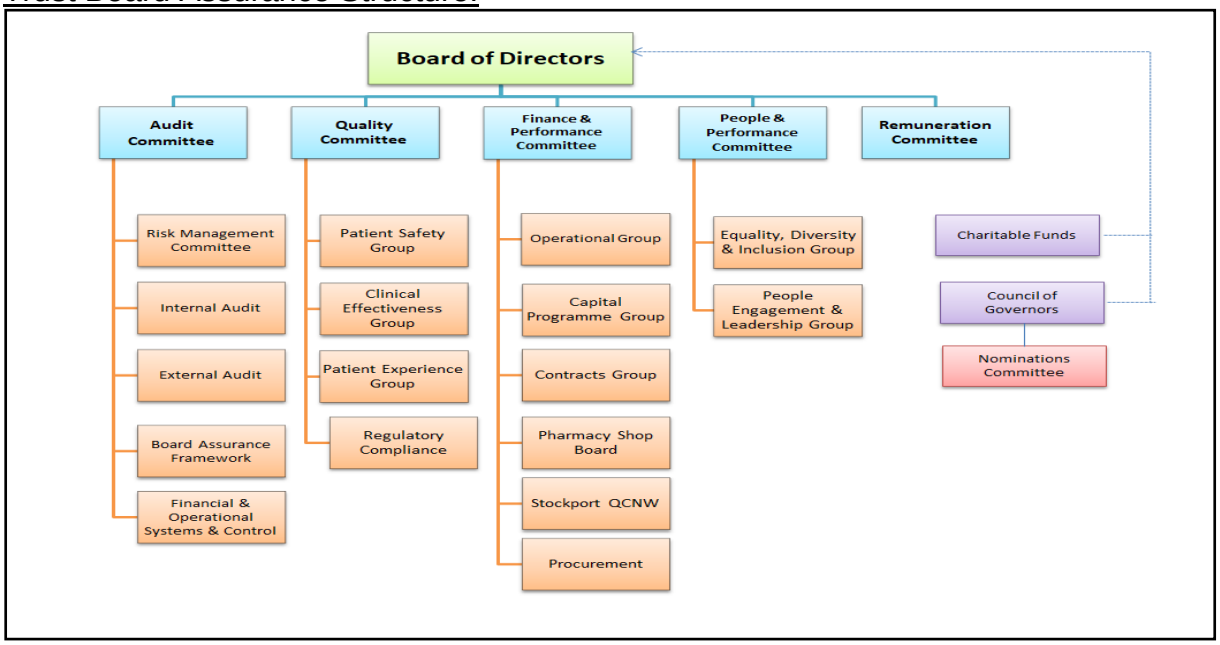
Appendix (A1): **Information Governance Management Framework**

Corporate Management Framework:



Appendix (A2): **Trust Assurance Framework**

Trust Board Assurance Structure:



Appendix (B): **Information Governance (Training Needs Analysis)**

Module Title	Estimated completion time	Staff Group: All Staff	Staff Group: IAO`s *	Staff Group: IAA`s **
Confidentiality & Caldicott				
The Caldicott Guardian in the NHS and social care$^{\Omega}$	1 Hour	Optional	**Mandatory**	Recommended
Access to Health Records	30 Minutes	Recommended	Recommended	Recommended
Data Security (Information Governance):				
Data Security Awareness (Trust e-learning or paper Workbook)	30 minutes	**Mandatory**		
Access to Health Records Ω	30 Minutes	Recommended	Recommended	Recommended
Information Risk Management:				
NHS Information Risk Management: for SIROs and IAOs$^{\Omega}$	1 Hour	Recommended	**Mandatory**	**Mandatory**
Information Security:				
NHS Information Risk Management: for SIROs and IAOs$^{\Omega}$	30 Minutes	Recommended	Recommended	**Mandatory**

* Including the Senior Information Risk Owner (SIRO) and Caldicott Guardian, and also undertake specialist SIRO and Caldicott training, as required.
** Including Governance Division representatives, Information Governance & Security Group (IGSG)
† Mandatory Data Security Awareness /refresher training for all staff annually
‡ Mandatory for staff dealing with subject access requests e.g. medico-legal, medical records and x-ray staff.
ΩTo be repeated every three years

Paper Workbooks are available from I.G. Department by contacting information.governancer@stockport.nhs.uk.

Any paper workbook assessments, once completed, should be returned to the I.G. Department

Appendix (C): **Guidance on Legal and Professional Obligation**

The links below provide guidance on the following legislation and regulatory framework. The guidance outlines the impact of these provisions on NHS Trusts and information and identifies the trusts responsibilities and approach to meet these requirements.

NHS Information Governance - Guidance on Legal and Professional Obligations

The Department of Health provided a guidance document for Trusts in relation to legal, regulatory and professional obligations, which included the following:

- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Common Law Duty of Confidentiality
- Human Rights Act 1998
- Freedom of Information Act 2000
- The Re-use of Public Sector Information Regulations 2005
- Environmental Information Regulations 2004
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- The Access to Medical Reports Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1990
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Public Interest Disclosure Act 1998
- The Public Records Act 1958
- Administrative Law
- NHS Act 2006
- Road Traffics Act 1988
- Regulations under Health and Safety at Work Act 1974
- Human Fertilisation and Embryology Act 1990
- Abortions Regulations 1991
- NHS Trust and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000
- Confidentiality: NHS Code of Practice 2003
- Information Security Management: NHS Code of Practice 2007

Please view the link below for further information on each legal, regulatory and professional obligation:

https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations