Stockport
NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY POLICY

CONTENTS AND PAGE NUMBERS

EXECUTIVE SUMMARY

Stockport NHS Foundation Trust has a legal obligation to comply with all appropriate legislation in respect of Data Protection and Information Security. It also has a duty to comply with guidance issued by the Department of Health, NHS Digital , the General Medical Council (GMC), the Information Commissioner's Office (ICO), as regulator of the Data Protection Act (DPA) together with the UK General Data Protection Regulations (GDPR), and other advisory groups to the NHS as well as other professional bodies.

This Data Protection & Confidentiality Policy (the Policy) aims to detail how Stockport NHS Foundation Trust meets its legal obligations, NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 2018 which is the key piece of legislation covering security and confidentiality of personal information.

For the purpose of this policy other relevant legislation and appropriate guidance may be referenced. A brief summary of the Data Protection Act, associated legislation and guidelines are detailed in Appendix 1.

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 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.

All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to Stockport NHS Foundation Trust. This relates to roles that are reliant upon computer systems such as: patient administration, payment/purchasing, invoicing, treatment planning and, audit and research. Legislation also regulates the use of manual records relating to patients, staff and others whose information may be held by Stockport NHS Foundation Trust or its employees.

Penalties could also be imposed upon Stockport NHS Foundation Trust, and individual employees for non-compliance with relevant legislation and NHS guidance. These may include financial penalties, up to 4% of Gross turnover or €20M, whichever is greater,

being imposed on the organisation for serious breaches or criminal prosecution, including possible custodial sentences against individuals who knowingly, recklessly or deliberately misuse personal data (DPA 2018, Part 6 – Enforcement, Para 170).

ROLES AND RESPONSIBILITIES

Chief Executive Officer (CEO):

The Chief Executive Officer has overall responsibility, as Accountable Officer, for Data Protection within Stockport NHS Foundation Trust.

Medical Director / Caldicott Guardian:

The Caldicott Guardian is a senior person responsible for safeguarding the confidentiality of patient and service-user information and enabling appropriate information-sharing. They play a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

The Caldicott Guardian should authorise disclosure of personal information relating to patients where the data subject has not consented to the disclosure.

Head of Information Governance and Security / Data Protection Officer (DPO):

The Head of IG / DPO is the designated Trust Data Protection Officer and is responsible for ensuring compliance with the data protection act and associated legistation.

They are responsible for coordinating improvements in data protection, confidentiality and information security and compliance with NHS Data Security and Protection Toolkit annual assessment.

They will ensure that records of processing activities including an information asset register of all applications/databases is maintained.

Information Governance & Security Group:

The implementation of, and compliance with, this Policy is the responsibility of the Information Governance & Security Group. Other designated personnel and managers across the Trust should also take responsibility for ensuring compliance with this policy.

Chief Finance Officer / Senior Information Risk Owner (SIRO):

The SIRO takes ownership of the risk management of information assets and assures risk assessment process to the Board and is responsible for advising the Chief Executive Officer on information related risks.

Information Asset Owners (IAO's):

IAO's are operationally responsible at senior levels for all information assets within their business 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 at least an annual basis of review.

Information Asset Administrators (IAA's):

IAA's work at local business/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. This includes notifying the Information Governance Team / DPO of any applications / databases that have not previously been registered.

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 responsible 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 are responsible for any records or data they create and what they do with information they use.

All staff must undertake the mandatory data security awareness training on an annual basis to maintain their knowledge and skills.

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

All staff and managers who have responsibilities for those staff must ensure that they abide by this policy.

GLOSSARY OF TERMS

Consent

The data subject's consent shall mean any **freely given**, **specific**, **fully informed** and **unambiguous** indication of his/her wishes by which the data subject signifies his/her **agreement** to personal data relating to him/her being processed. (Data Protection Act 2018, Part 4, Chapter 1, para 84 [2])

Personal Data

Any information relating to an identifiable living individual who can be directly or indirectly identified in particular by reference to an identifier, including name, address, telephone number, identification number, location data or online identifier.

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. This includes the nationally recognised NHS number.

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.

This is wider than, but includes, data defined as 'special category' under the Data Protection Act 2018. In addition to personal and clinical information, financial and security information is also likely to be deemed "special category".

Examples of special category data include information in relation to a person's:

- Health, physical and Mental Health condition
- Sexual life
- Sexual Orientation
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions*
- Trade Union Membership
- Biometric data
- Genetics

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

(* criminal convictions is not specifically special category data but is treated the same way)

Database/System/Application

Where the term database/system/application is used in this policy it means any collection of person-identifiable or confidential information that can be processed by automated means. A few examples are detailed below:

- Patient records (names and addresses etc.) for appointments
- Patient details used for prescribing drugs
- Patient information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this could be an Excel spreadsheet
- Staff records held on Excel to monitor annual leave and sickness

Information Asset

Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation. All databases/systems and applications are Information Assets that are recorded and reviewed within the Trust Information Asset Register.

Data Controllers

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used. As data controllers, employers have a responsibility to establish workplace practices and policies that are in line with the Act.

Data Users

Data Users include employees whose work involves processing personal information. As a data user, you have a legal duty to protect the information you handle. You must follow your employer's data protection and security polices at all times.

Data Subjects

Data Subjects are the people to which the data relates to. Within the workplace, they may be current employees, people applying for jobs or former employees. Data subjects might also be customers, suppliers, clients, patients, former patients or other people information is held about.

Data Processors

Data Processors may be separate organisations who process information on behalf of data controllers. They must also follow the Act and make sure information is handled properly.

Data

Data is recorded information, whether stored electronically on computer or in paper based filing systems.

Processing

Processing is any activity that involves the data. This includes collecting, recording, retrieving or retaining the data, or doing work on the data such as organising, adapting, changing, transmitting, erasing or destroying it.

THE PROCESS

PART ONE

Data Protection Principles

The Data Protection Act (2018) has seven principles of good practice.

Principle 1 - Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals

Principle 2 - Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Principle 3 - Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Principle 4 - Accuracy

Personal data shall be 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

Principle 5 - Storage limitation

Personal data shall be 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

Principle 6 - Integrity and confidentiality (security)

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

Principle 7 - Accountability

The controller shall be responsible for, and be able to demonstrate compliance to obligations and principles.

Processing Requirements

There is a requirement under principle one to make the general public, who may use the services of the NHS, aware of **why the NHS needs information about them, how this is used and to whom it may be disclosed**. Stockport NHS Foundation Trust is obliged under the Data Protection requirements and Caldicott recommendations to produce patient information leaflets and posters which are customised to its own use/s of personal information.

This also applies to information about employees. There must be procedures to notify staff, temporary employees (volunteers, locums) etc. of the reasons **why their information is required, how it will be used and to whom it may be disclosed.** This may occur during induction or by their individual manager.

This information is known as providing a Fair Processing Notice and these notices are available on the Trust website.

Patients will be made aware of this requirement by the use of information posters in patient waiting areas, statements in patient handbooks/on survey forms and verbally by those health care professionals providing care and treatment. Patient information leaflets and posters have been produced and are available upon request and sited in patient areas.

Considerations should be given to individuals whose first language is not English or who have learning or reading difficulties. Leaflets can be made available in various formats and languages when required; details are included within the leaflet.

Staff have a duty to inform patients about how their information is used in order to provide them with high quality health care. This might involve sharing their information between members of care teams, with other organisations involved in healthcare or with non-NHS organisations. This might also involve clinical audit, which is a legitimate component of healthcare provision, but this might not be obvious to patients and should be drawn to their attention.

Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume/rely on implied consent. Additional efforts to gain explicit written consent are required or alternative approaches that do not rely on identifiable information, such as the use of anonymised information, need to be developed.

You must be clear about identifying the purpose(s) for any processing of personal data. The same file of data may be used for several different purposes, but you must identify all the purposes for processing. All processing must then be undertaken strictly within the purposes identified. **Any new processing must be declared before it goes ahead in accordance with principle two.** This would include notifying the data subject of any new/additional purposes.

Lawful basis for processing personal data

The lawful basis for processing personal data are set out in Article 6 of the GDPR.
At least one of these must apply when processing personal data:

(a) Consent: the individual has given clear consent for to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the individual, or because they have asked to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for an official function, and the task/function has a clear basis in law.

(f) Legitimate interests: the processing is necessary the legitimate interests of the data controller a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to a public authority processing data to perform an official task.)

As a public authority, the Trust would rely primarily on the public task condition (e) for processing personal data.

Lawful basis for processing special category data

A lawful basis for processing under Article 6 would still be required as for personal data but would also need to satisfy a specific condition under Article 9 as it is more sensitive, and so needs more protection.

At least one of these must apply when processing personal data:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

(b) processing is necessary for the purposes of carrying out obligations in the field of employment and social security law and social protection

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is incapable of giving consent;

(e) processing relates to personal data made public by the data subject;

(f) processing is necessary for establishment, exercise or defence of legal claims

(g) processing is necessary for reasons of substantial public interest,

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

(i) processing is necessary for reasons of public interest in the area of public health

The Trust would rely primarily on the medical purposes condition (h) for processing special category (health) data.

Adequacy and Relevance

Information collected from individuals should be complete and should all be justified as being required for the purpose they are being requested.

Unnecessary data items should not be collected and each data item used should be fully justified. It also helps to only record facts and avoid personal opinions.

Consent

Under Data Protection Act 2018 and the UK General Data Protection Regulation, the legal basis which allows the Trust to collect, process and share patients' information is :
Article 6(e) - Public Task: the processing is necessary to perform a task in the public interest or for an official function and the task or function has a clear basis in law and;
Article 9(h) – the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

Explicit consent is therefore not usually required for sharing information needed to provide healthcare.

Many current uses of confidential/person identifiable information do not contribute directly to the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society - e.g. medical research, protecting the health of the public, health service management and financial audit. However, as they are not part of the 'medical purpose', we cannot assume that patients are content for their information to be used in these ways. Staff must therefore obtain explicit written consent before using information in this way.

Consent is not usually required for processing information as required by law. This would include employment obligations/rights, such as payroll, processing which takes place for the prevention of fraud and processing information for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment. This may include information of the following nature:

- racial or ethnic origin;
- religious beliefs or other beliefs of a similar nature;

- physical or mental health or condition

Data subjects generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right.

Staff must:

a. Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care
b. Check that patients and staff understand how their information is to be used and answer any concerns or queries
c. Respect patients' and staff decisions to restrict the use or disclosure of information. Where such decisions may compromise the delivery of healthcare, careful discussions with the patient are required. This should then be recorded on the patient's notes.

Registration and Notification

All purposes for processing person-identifiable or confidential information about living individuals must be registered with the Information Commissioners Office (ICO). This process is known as notification.

The DPO will maintain the Trust's Data Protection registration.

Information Asset Owners (IAO) and Information Asset Administrators (IAA) should ensure that the DPO is made aware on any new/additional databases, systems or applications that are introduced to their department/service. A nominated person will be responsible as an Information Asset Owner (IAO) and/or Information Asset Administrator (IAA) for each registered database, system or application. A log of databases/systems/applications and nominated Information Asset Owners (IAO) and Information Asset Administrators (IAA) will be maintained by the DPO .

Accuracy and Data Quality

Stockport NHS Foundation Trust has to ensure that all information held on any media is accurate and up to date in line with principle four. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

Users of computer systems will be responsible for the quality (i.e. accuracy, timeliness, and completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

Staff should check with patients that the information held by Stockport NHS Foundation Trust is kept up to date by asking patients attending appointments to validate the information held. Including demographic information (name and address), GP details, Next of Kin/Emergency Contact and NHS Number. See the Trust's Data Quality Policy for further information.

Staff should also confirm the accuracy of records through comparison with other records.

Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/Personnel department. This may also include asking employees to validate information for equality monitoring purposes, for example age, ethnicity, religion, gender, disability, sexual orientation.

Retention of Information

The NHS Records Management Code of Practice provides comprehensive guidance for Health Authorities and Trusts and includes a full retention schedule detailing retention periods for all types of records. Compliance with this guidance will help to ensure compliance with principle five of the Data Protection Act. All records are affected by this procedure regardless of the media they may be held, stored, retained. See the Trust's Information Lifecycle and Records Management Policy for further information.

If the information on the computer or manual record is not the main record, this is considered to be transient data, and procedures must be put in place to give guidance to these users that the information should be culled, archived or destroyed when no longer deemed to be of use.

Subject Access

Under Article 15 of the General Data Protection Regulations (Section 45 of the Data Protection Act 2018), individuals have the following rights:

- right to be informed
- right of access
- right to rectification
- right to take erasure
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision-making and profiling

Some of these rights have to be determined by the courts. Exemptions may also apply in some circumstances.

Included in these rights is the right of Subject Access - Individuals whose information is held by Stockport NHS Foundation Trust have rights of access to it, regardless of the media which the information may be held/retained on. Individuals also have a right to complain if they believe that Stockport NHS Foundation Trust is not complying with any other of the requirements of the Data Protection legislation.

Stockport NHS Foundation Trust must ensure an up to date procedure is in place to deal with requests for access to information. Further details can be found in the Access to Personal Information (Subject Access) Policy and Medico Legal Procedures.

Compensation - Individuals have a right to seek compensation for any breach of the Act which may cause them damage and/or distress.

Complaints - Stockport NHS Foundation Trust will ensure the complaints procedures take account of complaints which may be received because of a breach or suspected breach of the Data Protection Act 2018.

Disclosure of Personal Information

It is important that information about identifiable individuals (such as patients and staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

All disclosures of person identifiable information should be recorded and processed in line with the Access to Personal Information (Subject Access) Policy.

Some disclosures of information may occur because there is a statutory requirement upon Stockport NHS Foundation Trust to disclose e.g. with a Court Order, because other legislation requires disclosure (tax office, pension agency - for staff and notifiable diseases - for patients).

Information should only be disclosed with the data subject's consent unless the disclosure is required by law or in the public interest. Caldicott Guardian approval should be sought where required.

Security

General Security

All information relating to identifiable individuals must be kept secure at all times. Stockport NHS Foundation Trust will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to information. Further details of how this occurs can be found in the Information Security Policy.

Stockport NHS Foundation Trust will ensure the confidentiality, integrity and availability of data by implementing security controls and good work practices.

Staff should ensure that person identifiable data, whether in **manual form or electronic,** is not taken offsite unless authorised to do so and that it is done in an approved secure manner e.g. encryption or physically protected. This includes personal data that may be recorded in diaries which is often over-looked.

Where information is taken offsite, in particular manual records, it must be kept securely until it can be returned to a Trust work base. Identifiable information/Records must be transported securely i.e. in the boot of a car and not left on display; Identifiable information/records must be contained within a suitable, lockable container; Identifiable information/Records **MUST NOT** be left in a vehicle overnight. The information must be removed from the vehicle into the security of a dwelling. Staff transporting Trust medical records are advised that, where necessary and/or in an emergency (for example in the

case of staff sickness), arrangements must be made to return the information to a Trust member of staff.

All removable media & mobile devices holding Stockport NHS Foundation Trusts data must be encrypted. Staff are responsible for informing Digital Technology & Support (IT services) if they become aware of a device that has not been encrypted. See the Mobile Devices and Removable Media Security Policy for further information.

Staff should be made aware of and comply with the Information Sharing & Transfer of Records Policy & Guidance issued by the Trust's Information Governance department which are all available on the Information Governance & Security micro-site on the Trust Intranet.

Information, including personal and clinical information relating to patients or staff, must not be stored locally on any Trust PC or mobile device.

Identifiable Patient Information should not normally be circulated within the Trust using internal post/mail. It is a requirement that patient information is accurately tracked and using internal mail makes this impossible. It is the responsibility of users to ensure that information is returned securely (for example either Secretary to Secretary or back to Health Records Library) and information which forms part of a patient's medical record should be delivered direct and not via the internal mail.

Adequate alternative data security arrangements should be implemented when normal working practices cannot be followed.

Stockport NHS Foundation Trust has a legal obligation to maintain confidentiality & security standards for all information relating to patients, employees and Stockport NHS Foundation Trust business. It is important that this information is disposed of in a secure manner.

Measures should be taken to ensure that confidential paper waste is securely shredded or is collected and held in a secure area prior to disposal in line with the Trust's confidential waste policy.

System Security

Each system must have a designated Information Asset Owner (IAO) and Information Asset Administrator (IAA) who as part of their responsibilities must complete a system level security procedure and ensure that:

- that the system and its users comply with the current Data Protection legislation and with the Data Protection Principles;
- the Data Protection registrations/notifications are up to date;
- disclosures of information are checked against the registrations;
- unusual requests for the disclosure of information are scrutinised ;
- staff are aware of their responsibilities regarding security, data protection and confidentiality issues;
- that procedures are in place to achieve a high level of data quality.

Security of Paper Diaries

Only pertinent information should be recorded in diaries and only the absolutely minimum amount of personal data should be used. Clinical details, dates of birth and Lorenzo or NHS numbers must not be recorded in diaries.

Information contained in diaries must comply with the requirements of the Trust's Information Lifecycle and Records Management Policy. Personal opinions should not be recorded and abbreviations should not be used.

Diaries are the property of the Trust not the individual professional; and may be accessed at any time to be checked by authorised staff e.g. internal audit; or by the Counter Fraud & Security Management Service (CFSMS).

Patient information contained in diaries should not be altered once completed. If any entry is later found to be inaccurate, misleading or misreported the mistake should be crossed out using a single line, the date and time that the alteration was made should be recorded; and the correction should be signed. The deleted entry should remain legible. Snopake/Tippex, or self adhesive labels to cover entries, should never be used to alter a paper diary.

Diaries containing personal information should not be left unsecured overnight; nor in any "open" work area during working hours; unless they are being actively used for planning patient care. If staff leave the room, the diary must be put in a locked drawer/cabinet or the door locked. Appointment diaries must not be shown to patients.

Diaries or any other paper records containing personal data should not be taken home at night, unless justified and risk assessed by an appropriate manager. Where the taking home of diaries has been authorised they should not be left in a car overnight; but taken into the house with steps taken to safeguard personal and patient information and to ensure they cannot be read by any unauthorised person.

Diaries are an official record and need to be kept for 2 years and disposed of securely when no longer required. On resignation / retirement, diaries should be handed to the employees line manager.

It is important that diaries can be retrieved at any time during the retention period, whether for management or legal purposes. Any loss of a diary should be reported in line with the Trust's incident reporting procedure and should also be reported to the Information Governance team.

Passwords and door-codes should not be recorded in diaries.

These principles apply to both paper and electronic diaries

Data Sharing

All third parties organisations and suppliers that may have access to or process Stockport NHS Foundation Trust person-identifiable/confidential data must sign the Trust's latest data processing agreement or information sharing agreement and the requirements of this

agreement should be disseminated to the third parties employees. Individual confidentiality agreements should also be signed by third party employees or contractors.

All data sharing arrangements must comply with the Information Commissioners Office Data Sharing Code of Practice.

An Information Sharing Protocol must be completed for all data sharing activities and signed by all parties participating. See the Information Sharing and Transfer of Records Policy for more information.

If person identifiable information/records need to be transported on any removable media or mobile devices such as CD/DVDs, USB memory sticks, portable hard disks, tablets or manual paper records, this should be carried out to maintain strict security and confidentiality of this information, including suitable encryption. See the Information Sharing & Transfer of Records Policy, Mobile Devices and Removable Media Security Policy and associated guidance for further information.

Reliable and secure transport couriers should be used at all times. Packaging should be sufficiently robust and sealed to protect the contents from any physical damage or security breaches during transit, and should be in accordance with manufacturers' specifications.

Overseas Transfers

If you need to send person identifiable information to countries outside of the UK or EEA you must discuss this with the DPO as the levels of protection for the information may not be as comprehensive as those in the UK. The International Data Transfer Agreements (IDTA) and Standard Contractual Clauses (SCCs) should be incorporated in Data Processing Agreements and appropriate security measures in place.

Where electronic information is concerned you may need to check with software suppliers to ensure they conduct any development and bug fixes etc. within the UK or EEA.

Since the UK left the EU on 31/12/2020, an adequacy decision approved by the European Court of Justice has been put in place to ensure the free flow of personal data between the EEA and UK until 2024.
Otherwise, alternative transfer mechanisms and assurances (Inc. IDTA and SCCs) should be sought from suppliers in the EEA to safeguard free flow of EU to UK personal data.

Data Protection Impact Assessment (DPIA)

A DPIA is a process mandatory under the GDPR/Data Protection 2018 legislation when considering changes to or introducing processing of high risk identifiable data, which helps assess the privacy risks to individuals in the collection, use and disclosure of information. DPIAs help identify privacy risks, foresee problems and bring forward solutions and ensure compliance with the Data Protection Act.

This document must be completed for any new / or change in service which pertains to utilise person identifiable information and submitted to the Information Governance Team for review and approval, including to the Information & Security Group (IGSG), as required.

Where a processing activity is found to be high risk and it is not possible to mitigate the risk, the Caldicott Guardian and SIRO should be advised along with the Information Commissioner, who has the power to ban the processing.

Research

Where person identifiable data is to be collected for research purposes the following must be in place before commencement of the research and any data collection:

- Health Research Authority (HRA) approved Patient Information Sheet explaining what data will be collected and who will have access;
- HRA approved Informed Consent Form; and
- NHS Permission letter for the research project, issued by the Trust Research & Development (R&D) Office

Staff Training & Awareness

- **Training** - The Chief Executive, supported by the Data Protection Officer, Caldicott Guardian and SIRO has overall responsibility for maintaining awareness of data protection, confidentiality and security issues for all staff. This is carried out through the mandatory training sessions via e-learning and classroom based sessions and on-going awareness and evaluation campaigns/communications covering the following subjects:

- Personal responsibility
- Confidentiality of personal information
- Relevant Stockport NHS Foundation Trust Policies and Procedures
- Compliance with the Data Protection Principle and Caldicott Guardian Principles
- Individuals rights (access to information and compliance with the principles)
- General good practice guidelines covering security and confidentiality
- All staff completing the Trust's mandatory training are made aware of who the DPO, Caldicott Guardian and SIRO is and how these named staff can be contacted to raise any problems/concerns which may occur in the areas of security and confidentiality of personal information

Induction - All new starters to Stockport NHS Foundation Trust will be given details of how to access an online platform that has been created by Training department for all new starters. The platform includes awareness information of Data Security, and states that all staff have a legal duty to protect patient and staff personal information. They are also provided with details of different options on how to complete Data Security Awareness training and that this has to be completed within thirty days of employment which is in line with our Information Governance policy.

None compliance within the first thirty days of employment will be monitored by the monthly reminder email from Information Governance to staff who are not compliant.

New starters are also instructed to review the Information Governance pages which are on our Intranet, these pages outline key IG policies and guidance for staffs expected working

practices. Also upon logging in to the Trust's network users will be presented with the IT Acceptable Use policy declaration, which users should always read and comply with, as this is confirming that they accept their responsibilities in relation to Information Governance.

Staff who's role requires additional Information Governance training will be required to complete additional training by their managers.

Contracts of employment - Staff contracts of employment are produced and monitored by the Stockport NHS Foundation Trust Personnel/Human Resources department. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff are subject to the same rules.

All Stockport NHS Foundation Trust employees will be made aware of their responsibilities in connection with this Policy through their contract of employment, and targeted training sessions carried out by the information governance department, Information Asset Owner (IAO) or Information Asset Administrator (IAA) and/or other trainers/specialists.

Disciplinary - A breach of the Data Protection requirements could result in a member of staff facing disciplinary action / dismissal. A copy of these procedures is available from the Personnel/Human Resources Department/microsite.

Patient Information

There are specific requirements highlighted within the Caldicott recommendations that apply to patient identifiable information. These are also requirements of compliance with the Data Protection legislation. Specifically they relate to security, confidentiality and fair obtaining of information as well as ensuring all disclosures are valid and authorised.

All patient information, whether manually or automatically held, will be kept secure at all times and especially when not being used for patient care or related purpose.

Patients will be made aware of their right of access to their records.

The guidance relating to good handling practice for records is contained within the NHS Records Management Code of Practice.

Handling subject access requests made by, or on behalf of, a current or past patient will be dealt with by the Medico-Legal Department, Patient and Customer Services of Stockport NHS Foundation Trust. In some circumstances the Stockport NHS Foundation Trust Caldicott Guardian/Data Protection Officer may also be involved.

Stockport NHS Foundation Trust has appointed a 'Guardian' who will oversee disclosures of patient information with particular attention being paid to extraordinary disclosures (those which are not routine and without consent). This person will be known as the Caldicott Guardian and will oversee the guidance in the Caldicott Guardian Manual and NHS Code of Confidentiality.

Staff Information

Any member of staff current, past or potential (applicant) who wishes to have a copy of their information under the subject access provision of the Data Protection Act will need to contact, in writing, the Human Resources (HR) Department, Aspen House, Stockport NHS Foundation Trust. There are subject access procedures outlining the process to follow to deal with such requests.

Enforcement

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit.

The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

The tools are not mutually exclusive. The ICO will use them in combination where justified by the circumstances.

The main options are:

- serve **information notices** requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- issue **undertakings** committing an organisation to a particular course of action in order to improve its compliance;
- serve **enforcement notices** and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct **compulsory audits** to assess whether organisations processing of personal data follows good practice;
- issue **monetary penalty notices**, requiring organisations to pay up to up to 4% of the organisation's gross income (or £17.5 million, whichever is greater) for serious breaches of the Data Protection Act occurring on or after 25 May 2018 or serious breaches of the Privacy and Electronic Communications Regulations;
- **prosecute** those who commit **criminal offences** under the Act; and
- report to Parliament on data protection issues of concern.

Appeals from notices are heard by the First–tier Tribunal (Information Rights), part of the General Regulatory Chamber (GRC). The First–tier Tribunal (Information Rights) specifically hears appeals of enforcement notices, decision notices and information notices issued by the Information Commissioner. The GRC brings together a range of previously separate tribunals that hear appeals on regulatory issues.

Associated Legislation

Privacy and Electronic Communications Regulations (PECR)

The Privacy and Electronic Communications Regulations regulate direct marketing activities by electronic means (by telephone, fax, email or other electronic methods). They also regulate the security and confidentiality of such communications, with rules governing the use of cookies and 'spyware'.

The Regulations complement the Data Protection Act 2018 (DPA) in the regulation of organisations' use of personal data and in ensuring appropriate safeguards for individuals' rights and privacy.

Part 5, Section 122 of the Data Protection Act 2018 provides the Information Commissioner's Direct Marketing Code advising that direct marketing is 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals'.

Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA regulates the powers of public bodies to carry out surveillance and investigation, and covering the interception of communications. It was introduced to take account of technological change such as the growth of the internet and strong encryption.

RIPA can be invoked by government officials specified in the Act on the grounds of national security, and for the purposes of detecting crime, preventing disorder, public safety, protecting public health, or in the interests of the economic well-being of the United Kingdom.

Human Rights Act 2000 (HRA)

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each user an individual user id and password which will only be known by the individual they relate to

and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. The penalties for breaching the computer misuse act include up to five years imprisonment.

Freedom of Information Act 2000 (FOI)

The Information Commissioner also oversees the implementation of this Act. This Act gives individuals rights of access to information held by public authorities. Further information is available in the Trust's Freedom of Information Act policy.

Gender Recognition Act 2004

The Gender Recognition Act refers to 'protected information' about transsexual people. The purpose of the law is to recognise that there are legitimate times when people do need to know about a transsexual person's gender reassignment in order to do the best and right thing. The law is not there to enforce absolute secrecy but to remind officials that they have a serious responsibility for the potentially negative outcomes of using information irresponsibly.

Section 22 of the Act says that: 'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.' 'Protected information' means information which relates to a person who has made an application under the Gender Recognition Act. This covers both the fact of the application itself and, if the application was successful, the fact that the individual was previously of the opposite gender to the one in which they are now legally recognised.

The Equality Act 2010

The Equality Act harmonises and replaces previous legislation (such as the Race Relations Act 1976 and the Disability Discrimination Act 1995) and ensures consistency. The Act covers the same groups that were protected by previous equality legislation – age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity. These are now called 'protected characteristics". It extends some protections to characteristics that were not previously covered, and also strengthens particular aspects of equality law to help tackle discrimination and inequality.

PART TWO - CONFIDENTIALITY CODE OF CONDUCT

Confidentiality is fundamental to patient care and the employment of staff. Any breach of confidentiality to an unauthorised person, however innocently made, must be treated seriously, in line with the Trust's disciplinary procedures.

The Caldicott Principles

The general principles underlying the use and sharing of patient identifiable information are known as the Caldicott principles. The name comes from the original report into confidentiality in the NHS in 1997, known as the Caldicott Report.

There are eight Caldicott principles as laid down by the NHS Executive to improve the handling and protection of patient information from the 2012 review and further review in 2020, undertaken to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of patient information to improve patient care.

1. **Justify the purpose(s) -** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary -** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data -** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis -** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities** - Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law -** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality -** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8. **Inform patients and service users about how their confidential information is used**
   A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential

information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

There is also a Caldicott Guardian who is the Executive Director with responsibility for confidentiality. In Stockport NHS Foundation Trust this is the Medical Director.

These are useful if you are unsure about whether or not to disclose information to someone. If the purpose of using the information does not form part of the patient's care and treatment, or you feel that too much information is being requested, then you should refuse to disclose the information.

An authorised person is an individual or organisation designated by statute or by the Trust.

As a result of the diverse nature of services provided at Stockport NHS Foundation Trust, Divisions may have separate supplementary and complementary local policies and procedures. Anyone with access to Trust information has a responsibility to establish if such policies and procedures are in place.

Patients

All patients have the right to expect complete confidentiality in relation to their care and treatment. It is a breach of confidentiality to:

(i) disclose to an unauthorised person the fact that a patient has been identified as being on the premises;
(ii) disclose to an unauthorised person any detail about a patient's condition, treatment, or any other detail about a patient gained in the course of working within the Trust;
(iii) use information gained about patients in the course of working within the Trust for purposes other than those genuinely connected with the care and treatment of the Trust's patients.

All those working within the Trust must therefore ensure that they **do not**:

(i) divulge confidential information concerning patients to unauthorised persons;
To this end, Patient healthcare records must be kept secure at all times and not left unsecured in a public place. The Trust has made arrangements to ensure that staff are able to comply with this requirement for example the provision of lockable medical records trollies for the Wards.

With regard to patient identifiable information on Ward Whiteboards, it is Trust policy that only surnames are used (the exceptions to this are where there are two patients with the same surname when an initial can be used **by exception**, ED and Paediatrics who may use a first name and an age). This requirement relates also to the smaller side-room Whiteboards but does not apply to whiteboards above a patient's bed when the full name can be used.

The use of symbols to denote condition is acceptable, however the corresponding

legend must be kept away from public view – ensuring that all patient information is confidential and not available for inappropriate access by other patients/patient relatives.

(ii) discuss confidential information concerning patients in a way which might lead to accidental disclosure in public areas, such as corridors, lifts, dining areas or recreational areas within the Trust's premises;
(iii) discuss confidential information concerning patients outside the Trust's premises in a way which might lead to unauthorised persons gaining such information;
(iv) use information gained about patients in the course of working within the Trust for their own purposes
(v) access or look at any healthcare or personal information relating to themselves, in any circumstances, or that relating to family, friends or acquaintances unless directly involved in the patient's clinical care or management. In such circumstances the user must only access information if required to as part of their role. Where a member of staff accidentally accesses information inappropriately, by selecting the wrong record for example, such access must be reported to the line manager.

All those working within the Trust must equally ensure that **they always**:

(i) refer enquiries from the media to the Communications Manager in the first instance, or to a Senior Manager in the Division. Outside normal working hours, press enquiries should be reported to the Director on call.
(ii) refer enquiries about patients from police, solicitors or other agencies and organisations to their manager in the first instance, who should refer the request to the Medico Legal Department (Patient & Customer Services), the Information Governance Team or the Caldicott Guardian as appropriate. Outside normal working hours staff may need to contact the Director on call.
(iii) ensure Caldicott Guardian approval is obtained prior to disclosing patient information where the data subject's consent has not been provided.
(iv) refer to their manager for advice in situations in which a breach of confidentiality may have potentially occurred, either by themselves or by others;
(v) recognise the confidential and sensitive nature of patients' Health Care Records. Health Care Records must be stored and handled with care and discretion.

When an individual has died it is unlikely that information relating to that individual remains legally confidential. However, an ethical obligation to the relatives of the deceased still exists and health records of the deceased are public records governed by the provisions of the Public Records Act 1958 and the Access to Health Records Act 1990, which permits the use and disclosure of the information within them in only limited circumstances. Therefore our obligations of confidentiality and the provisions in this policy still apply.

Further Information and guidance can be obtained in the Access to Personal Information (Subject Access) Policy or by contacting the Information Governance Department.

Formal Correspondence with patients and other hospitals

All person identifiable and confidential/clinical information must be marked “confidential” and handled in line with the Information Sharing and Transfer of Records Policy. Correspondence must always be securely sealed and clearly addressed to a named contact. Placing a signature across the seal may help to avoid persons other than the addressee opening the envelope.

If information does not fall into these categories then ‘confidential’ should not be used.

Receipt of enquiries about patients

When requests are received seeking information about patients in the Trust, such information will not be disclosed without the prior permission of the patient. Local arrangements will have to be developed to ensure those with legitimate concerns have access to information.

Where, in the judgement of an Executive Director of the Trust, the failure to release the information would be contrary to the public interest, the NHS, or the interest of the patient concerned, information may be released under the provisions of the Data Protection Act 2018, and in line with the Access to Personal Information (Subject Access) Policy.

Where telephone or face-to-face enquiries are seeking information about patients, the person receiving the enquiry will establish the identity of the enquirer before person identifiable details are given. If the identity of the caller cannot be established the person receiving the call should take a note of the caller’s name and number and pass this on to the patient.

If the caller is from another hospital or GP and is seeking information which may affect the care of the patient, the identity of the enquirer must be confirmed and if there is any uncertainty, a return call must be made to a known contact number or switchboard in order to confirm the callers' identity. If there remains any doubt, this should be referred to a Manager in the Division.

Media enquiries requesting information about patients in the Trust should be referred to the Communications Manager or a Senior Manager in the Division.

Further information, clarification or advice about patient confidentiality can be sought from the Trusts Caldicott Guardian or Information Governance department.

Employees

All employees of the Trust have the right to expect that details of their employment with the Trust will be held in confidence. It will therefore be a breach of confidentiality to:

(i) disclose to an unauthorised person any detail relating to the person’s employment, or any other information about an employee gained in the course of working within the Trust;
(ii) use information gained about an employee in the course of working within the Trust for purposes other than those genuinely connected with the Trust’s business.

Information will only be disclosed with the express permission of the employee, except where in the judgement of an Executive Director it would be prejudicial to the public interest, the Trust or the employee concerned not to release the information.

The only exception to this rule is where the Trust is required to disclose information by law. This might include the release of names and grading structures of staff under the Freedom of Information Act 2000. Please refer to the Freedom of Information Policy for more information.

All those working within the Trust must ensure that they do not:

(i) divulge confidential information concerning employees to unauthorised persons.
(ii) discuss confidential information concerning employees in a way which might lead to accidental disclosure in public areas within the Trust's premises;
(iii) discuss confidential information concerning employees outside the Trust's premises in a way which might lead to unauthorised persons gaining such information;
(iv) use information gained about employees in the course of working within the Trust for their own purposes including using access given as part of their role to look at any personal HR records relating to themselves or members of family, friends or acquaintances.
(v) this also applies if employees are attending the hospital as a patient

All those working within the Trust should equally ensure that they always:

(i) refer enquiries about staff from the media, police, solicitors, department of social security or other organisations/agencies to their Manager;
(ii) ensure approval is obtained from the Director of Human Resources prior to disclosing information where the data subject's consent has not been provided.
(iii) refer to their Manager for advice in situations in which a breach of confidentiality may potentially have occurred either in relation to things that they have done or those that they know other people have done.

Further information, clarification or advice about employee confidentiality can be obtained from the Information Governance Department.

Formal Correspondence with employees

Any correspondence addressed to an employee of Stockport NHS Trust which is of a personal nature must be marked "Private and Confidential – to be opened by addressee only".

It is the responsibility of individual members of staff to notify their manager of any change of address.

Request for financial references

Requests for financial references such as those from banks and building societies are processed by Payroll Services and will need to be supported by a signed approval for

disclosure from the employee. If such approval is not available, it must be obtained before any disclosure is made.

Data Security

Information about individuals is increasingly held on computers. It is essential that such information as well as all manual information is securely held.

Only authorised users should have access to confidential information, in accordance with the Information Security Policy and any other local guidelines.

Personal passwords are issued to protect the integrity of these details. It is implicit that employees protect their passwords; including regularly changing these and ensuring that passwords are never shared.

The same principles of confidentiality must apply to all forms of communication. All person-identifiable information sent by email, fax or any other method must comply with the Information Sharing & Transfer of Records Policy as well as the Safe Haven Procedure. Local arrangements may also be in place to ensure good practice is established if information about patients or employees is faxed/emailed etc. Given the difficulties in ensuring the confidentiality of faxed/emailed information local arrangements should restrict the use of faxes to urgent information & only permit email communications if encrypted to approved NHS standards. Please refer to the Information Sharing and Transfer of Records Policy.

Commercial Issues

Information about the operation of the Trust and its financial arrangements may be considered to be prejudicial to the Trusts commercial interests. The Trust also receives information from other organisations which we may be obliged to ensure remains confidential.

Employees should be particularly careful of using, or making public internal information of this nature, which may be prejudicial to commercial interests. This principle applies whether private or other public sector providers are concerned, and whether or not disclosure is prompted by the expectation of personal gain (see Standards of Business Conduct Policy). Consideration should also be given to the Freedom of Information Act and requests directed to the Information Governance department as appropriate. All Parties have the same rights under this legislation and therefore this does not prejudice the principle of fair competition.

Relations with the media

All staff should refer media enquiries regarding patients, staff and the Trust's business to the Communications Manager. Any issues relating to Government, Statutory or Trust Policy must be directed to an Executive Director.

Staff concerns

Employees wishing to raise concerns regarding patient care, confidentiality, or any other activities of the Trust, should follow the "raising concerns at work" policy (formerly the whistleblowing policy) situated on the Trust Intranet.

DECLARATION

THIS SECTION TO BE COMPLETED BY THE USER

All users are required to read and sign the following declaration:

I have seen, read and understood Stockport NHS Foundation Trust's Data Protection and Confidentiality Policy.

I understand the terms of the policy and agree to abide by them.

I understand that audits may monitor and record compliance with this policy.

I understand that any violation of this policy could result in disciplinary action, and possibly dismissal or criminal prosecution.

Signed: _____

Name: _____

Date: _____

(You may also be required to electronically accept that you have read and understood this policy)

TRAINING

All staff are required to complete the annual mandatory Data Security Awareness training

MONITORING COMPLIANCE

The Trust will regularly monitor and audit its Data Protection 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, Digital Informatics Group, Assurance Risk Committee and the Audit Committee, as appropriate.

The Information Commissioner may also mandate an audit upon the Trust at any time.

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 Information Governance 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

The responsibility of implementing this document, 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 Security Group.

This Policy will be reviewed annually or more frequently if appropriate to take into account changes to legislation that may occur, and/or guidance from the Department of Health, the NHS Executive and/or the Information Commissioners Office (ICO).

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 Digital Informatics Group. 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 Security Policy
Information Governance Incident Reporting/Management SOP
System Level Security Procedure
IT Acceptable Use Policy
Mobile Devices & Removable Media Security Policy
Remote Access & Mobile Working Policy
Photography/Video & Audio Records of Patients/Staff
Network Security Policy
Access to Personal Information (Subject Access) Policy
Data Quality Policy
Freedom of Information Policy
Information Sharing and Transfer of Records Policy
Information Lifecycle and Records Management Policy
Confidential Waste Policy
Disciplinary Policy
BS 10008 – Evidential weight and legal admissibility of electronic information
Data Protection Impact Assessment
Comments, Concerns, Compliments and Complaints

EQUALITY IMPACT ASSESSMENT

Office Use Only

Submission Date:	*27.03.24*
Approved By:	*IGSG*
Full EIA needed:	Yes/No

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

1	**Name of the Policy/SOP/Service**	Data Protection & Confidentiality Policy	
2	**Department/Division**	IM & T	
3	**Details of the Person responsible for the EIA**	**Name:** **Job Title:** **Contact Details:**	Joan Carr Information Governance Coordinator Joan.carr@stockport.nhs.uk
4	**What are the main aims and objectives of the Policy/SOP/Service?**	Stockport NHS Foundation Trust has a legal obligation to comply with all appropriate legislation in respect of Data Protection and Information Security. It also has a duty to comply with guidance issued by the Department of Health, Connecting for Health, the General Medical Council (GMC), the Information Commissioner's Office (ICO), as regulator of the Data Protection Act (DPA) together with the General Data Protection Regulations (GDPR), and other advisory groups to the NHS as well as other professional bodies.	

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

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a differential 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. Stockport Population Data: Largest age band 40 – 49	Positive Impact See general comments	

Carers	Trust Workforce: No Data It is unlikely to affect carers disproportionately. 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.	Positive 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 The 2011 census indicates that 18.4% of Stockport residents are living with a limiting long-term illness	Positive Impact See general comments	
Race / Ethnicity	Trust Workforce: BAME make up 16.18% It is unlikely to affect people of a particular gender disproportionately. People from Black, Asian and Minority Ethnic (BAME) backgrounds are more likely to experience serious complications from the virus	Positive Impact See general comments	
Gender	Trust Workforce: 79.9% female It is unlikely to affect people who have gender reassignment disproportionately. Stockport's population is split almost equally by gender (51.1% female, 48.9% male), which mirrors the national trend.	Positive Impact See general comments	
Gender Reassignment	Trust Workforce: No Data It is unlikely to affect people of a particular marital status disproportionately 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	Positive 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. 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.	Positive 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.	Positive Impact See general comments	

	2% fertility rate On average there are over 3,300 births to Stockport resident mothers each year.		
Religion & Belief	Trust Workforce: 52.47% Christian It is unlikely to affect people of any particular religion or belief disproportionately. The majority of Stockport residents are Christian (63.2% - down from 75% at the last census), which is 4% greater than the national average.	Positive 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 It is estimated that 5-7% of the UK population is LGB, which would equate to 15-21,000 people in the borough.	Positive Impact See general comments	
General Comments across all equality strands	All patients have the right to expect complete confidentiality in relation to their care and treatment. Respect patients' and staff decisions to restrict the use or disclosure of information.	Stockport NHS Foundation Trust has a legal obligation to comply with all appropriate legislation in respect of Data Protection and Information Security including Equality Act 2010, Gender Recognition Act & Human Rights Act	

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 the 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	04/01/2022
Date of Last Review	04/01/2022

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			0	How will it impact on recruitment of staff?	No Impact		

	Experience				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

Organisations must ensure that any third parties used to process or share personal confidential data with, will ensure the data is secure and confidential and a data processing or information sharing agreement will 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 Data Protection Impact Assessment (DPIA):

- Setting up a new process using personal confidential data (PCD) that identifies individuals.
- 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/GDPR.

Advice/Guidance on completing the screening questions or the full DPIA can be provided by the Information Governance (IG) Team by emailing details of the initiative to:

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 to process 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 currently used 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 as being 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	Data Protection & Confidentiality Policy
Version Number	V 8.2
Consultation	Information Governance & Security Group
Recommended By:	Head of IG & Security / DPO
Approved By:	Digital Informatics Group
Approval Date	26th March 2025
Next Review Date	March 2026
Document Author	Head of IG / 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
8.2	Mar 25	Mar 25	IG	Review, update of new starters Data Security Awareness training
8.1	Mar 2024	Apr 2024	IG	Review of EIA and update of Data Security Awareness training
8.0	Mar 2023	Apr 2023		Added titles to DP principles, referred to IAR. Changed title for SIRO. Changed reference to business groups to divisions.
7.0	Mar 2022	Mar 2022		Update of IT Services and titles
6.4	Mar 2021	Mar 2021		Update links, added eigth Caldicott Guardian principle, EU Exit arrangement details. Changed title of Head of IG/DPO
6.3	Mar 2021	Mar 2021		Review
6.2	Mar 2021	Mar 2021		Update of SIRO and Caldicott Guardian titles
6.1	Dec 2018	Dec 2018		Clarification on Consent under DPA 2018
6.0	Jun 2018	Jun 2018		New Data Protection Act 2018 and GDPR updates and legal basis for processing Inclusion of responsibility of staff to report accidental access Clarification of the requirements governing whiteboards/medical records
5.0	Jun 2016	Jun 2016		Refresh of policy
4.0	Jul 2014	Jul 2014		Appendix a) removed and minor amendments
3.3	May 2013	May 2013		Requirements around diaries expanded in light of the transfer of community services. Additional Caldicott Principle added in light of Caldicott2 review.
3.2	Nov 2012	Nov 2012		Updated reference to whistleblowing policy to reflect

				new name “raising concerns at work policy”.
3.1	Feb 2012	Feb 2012		Reference to Equality Act added.
3.0	Nov 2011	Nov 2011		Adopted the new Trust Policy format. Significant Changes Made.
2.0 (Final)	Apr 2010	Apr 2010		Various
2.0 (Draft)	Apr 2009	Apr 2009		Data Protection & Confidentiality Policy merged. Adopted the new Trust Policy format. Significant Changes Made.
1.0	Feb 2004	Feb 2004		Data Protection Policy Developed
1.0	Dec 2001	Dec 2001		Confidentiality Policy Developed

APPENDICES

Appendix 1 - Legislation:

The legislation listed below refers to issues of security and or confidentiality of personal identifiable information/data (see the Information Governance Guidance on Legal and Professional Obligations document on the Information Governance & Security microsite for more detailed information and summaries of each).

This policy focuses on the Data Protection Act 2018 (the Act), which although not the only piece of legislation impacting upon this policy is the key piece of legislation governing this area.

Data Protection Act 2018
UK General Data Protection Regulations
Access to Health Records 1990
Access to Medical Reports Act 1988
Human Rights Act 1998
Freedom of Information Act 2000
Environmental Information Regulations 2004
Re-use of Public Section Information Regulations 2005
Copyright, Designs and Patents Act 1988
Regulation of Investigatory Powers Act 2000
Crime and Disorder Act 1998
Computer Misuse Act 1990
Electronic Communications Act 2000

Criminal Justice and Immigration Act 2008
The Privacy and Electronic Communications (EC Directive) Regulations 2003
Coroners & Justice Act 2009
The Common Law Duty of Confidentiality
The Data Protection (Processing of Sensitive Personal Data) Order 2000
Medicine for Human Use (Clinical Trials) Regulations 2004

There are further Acts of Parliament that govern the disclosure/sharing of personal and/or identifiable information – some make it a legal requirement to disclose and others state that information cannot be disclosed. Examples of these Acts include the following:

Legislation to restrict disclosure of person identifiable information

Human Fertilisation and Embryology (Disclosure of Information) Act 1992
Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
Sexual Abortion Act 1967
Abortion Regulations 1991
The Adoption Act 1976

Legislation requiring disclosure of person identifiable information

Public Health (Control of Diseases) Act 1984
Public Health (Infectious Diseases) Regulations 1988
Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
Births and Deaths Act 1984
Police and Criminal Evidence Act 1984
Children and Adoption Act 2006

NHS & related guidance

The following are the main publications referring to security and or confidentiality of personal identifiable information/data.

Department of Health (DoH):
Records Management Code of Practice for Health & Social Care 2016
Confidentiality: NHS Code of Practice 2003
Information Security Management Code of Practice 2007
The Caldicott Guardian Manual 2017

Health & Social Care Information Centre Information Governance Toolkit
BS ISO/IEC 27000:2013 Information Security Management Standards
Sir Gus O'Donnell Report on Data Loss 2008
Thomas-Walport Report on Data Loss 2008
Sir David Nicholson's Letter to NHS CEO's (September 2008)
Research Governance Framework for Health & Social Care, Second Edition, 2005

Information: To Share Or Not To Share? The Information Governance Caldicott2 Review (April 2013)

Data Protection Act 2018/ UK General Data Protection Regulations

The UK General Data Protection Regulations is the EU regulation adopted by the UK, the Data Protection Act 2018 is the legislation implemented in the UK to legalise the requirements of the GDPR.

This Act applies to all person identifiable data held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll data , health records, other manual files, microfiche/film, pathology results, x-rays etc.

The Act dictates that data should only be disclosed on a need to know basis. Printouts e.g. patient hand-over sheets and other paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence and managed according to the Trust Disciplinary Procedures.

The Act requires Stockport NHS Foundation Trust to register its personal data holdings with the Information Commissioner's Office (ICO), identifying all the purposes for holding the data, how it is used and to whom it may be disclosed – this information is also required to be shared with our patients, and this is achieved via the Trust website and the Trust's Fair Processing Notice. Stockport NHS Foundation Trust and all individuals working for or on behalf of the Trust have a statutory duty to comply with the principles of good practice known as the Data Protection Principles.

All Stockport NHS Foundation Trust's applications/databases must be registered with the Information Governance department to enable the Trust's Data Protection registration with the Information Commissioner to be kept up to date. All applications/databases must comply fully with the Data Protection Act. This will primarily be achieved by adhering to the policies of Stockport NHS Trust and following the Data Protection Principles listed on page 7.

Under a provision of the Data Protection Act an individual can request access to their information; regardless of the media this information may be held/retained.