Our Ref: NG/RM/24325
Date: 1st October 2024

Nicola Griffiths
Deputy Director of Governance
North Staffordshire Combined Healthcare NHS Trust
Lawton House
Bellringer Road
Trentham
ST4 8HH

Reception: 0300 123 1535

Dear

Freedom of Information Act Request

I am writing in response to your e-mail of the 10th September 2024**.** Your request has been processed using the Trust's procedures for the disclosure of information under the Freedom of Information Act (2000).

Requested information:
The Transformation Directorate's website indicates that the NHS is increasingly using technology to support care, with such technologies including virtual wards, apps, remote monitoring technologies, patient portals, and telemedicine devices. Examples of technology being used to support children's care are provided on some Trusts' websites. A limited number of examples of how such technologies are being used to support children's care are also outlined on the Transformation Directorate's website. There appears to be no comprehensive database for the public to access which outlines the technologies and apps that are currently being used to support children's care.

The posts which I have read which discuss how the NHS is using virtual wards, apps, remote technologies, patient portals and telemedicine devices, provide no information concerning what parents and children are told about how their data will be used or whether parents are able to opt out of such technology use.

1. Please can you therefore provide details of
a. whether (as at August 2024) any of the following are used by the Trust to support children's care: telehealth and telemedicine technologies, MHealth apps, health information technologies, remote monitoring technologies, digital healthcare devices, wearable devices and telemedicine devices and/ or any other technologies designed to facilitate personalised medicine not detailed above.
b. The names/details of technologies being used.
c. The purposes for which such technologies are being used.
Combined Wellbeing Portal - Self-help and online referral
AttendAnywhere - Video Consultation

NB we are not asking for detailed information about the operation or implementation of these technologies, but merely the broad purposes for which they are being used.

2. In your Trust, please can you advise what information clinicians are given about how data collected by such technology is processed, for what purposes, and with whom it

is shared. Again, we are asking for information in broad terms e.g. whether information is shared with commercial entities/third parties and the status of those entities i.e. technology provider but not the names of those entities. **Broad guidance is provided as part of the technology deployment, the Digital team would consult on any specific guidance required by services.**

3. Please can you confirm what information doctors and other health professionals in your Trust give/are advised to give to child patients and/or their parents about the benefits and risks of using such technology generally/specifically. **Broad guidance is provided as part of the technology deployment, the Digital team would consult on any specific guidance required by services.**

4. Please can you confirm what information doctors and other health professionals in your Trust give/ are advised to give to child patients and/or their parents about how data collected by such technology is processed, for what purposes, and with whom it is shared. **Broad guidance is provided as part of the technology deployment, the Digital team would consult on any specific guidance required by services.**

5. Please can you provide copies of all policies and documents that have been developed by or within the trust with a view to ensuring that when NHS staff are advocating the use of such technology, children and parents' information is processed in accordance with the UKGDPR. **Data collection and information sharing is covered in the Trust privacy notice. https://www.combined.nhs.uk/about-us/privacy/**

   Broad guidance is provided as part of technology deployments and the Digital team would consult on any specific guidance required by services.

   All Trust employees are expected to follow Trust policies when dealing with patient data. Please see attached Appendices 1-3

6. Please can you advise what information is currently provided within your Trust for the child patients and their parents to refer to should they have any queries about how data collected by such technologies is used and by whom. **Broad guidance is provided as part of the technology deployment, the Digital team would consult on any specific guidance required by services.**

7. Please can you advise what advice is provided to clinicians in your Trust about the response they should give where a child patient or their parent does not wish to use such technologies/ wishes to opt out of data collection or sharing related to the use of such technologies.
   Broad guidance is provided as part of the technology deployment, the Digital team would consult on any specific guidance required by services.

   AttendAnywhere Video Consultation is offered to community patients, a face-to-face appointments are also offered as alternative should patient/ carer not wish to use this technology.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review of the management of your request. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Dr Buki Adeyemo, Chief Executive, North Staffordshire Combined Healthcare Trust, Trust Headquarters, Lawton House, Bellringer Road, Trentham, ST4 8HH. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

Nicola Griffiths
Deputy Director of Governance

Keele University Teaching Trust

NHS North Staffordshire Combined Healthcare NHS Trust

Doc level: Trustwide
Code ref:7.01

Confidentiality of Patient and Employee Information Policy

Lead executive	Chief Medical Officer
Authors details	Health Records & Information Governance Manager

Type of document	Policy
Target audience	All Trust staff and patients
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet its legal obligations under Data Protection legislation and NHS requirements concerning confidentiality of their information.

Approving meeting	Quality Committee	Meeting date	5th September 2024
Ratification date	5th September 2024	Review date	30th September 2027

Trust documents to be read in conjunction with	
Document code	Document name
4.18	Risk Management Policy
5.01	Incident Reporting Policy
7.02	Subject Access Request Policy
7.03	Information Security & Data Protection Policy
7.05	One Staffordshire Information Sharing Protocol

Document change history		Version	Date
What is different?	– This policy has been revised in line with legislation changes under the Data Protection legislation. –		
Appendices / electronic forms	–		
What is the impact of change?	– Making all staff aware of changes in legislation which impact on confidentiality – Ensuring that the Trust is compliant with its legal requirements under Data Protection and other associated legislation.		

Training requirements	There are no specific training requirements for this document. Confidentiality training is covered under the Data Security Awareness national training tool

Document consultation	
Directorates	
Corporate services	
External agencies	

Financial resource implications	No

External references
1. Data Protection Bill 2. General Data Protection Regulations (GDPR)

Monitoring compliance with the processes outlined within this document	Any breaches to this policy will be recorded within the Trust's incident reporting system and any breaches will be investigated accordingly.

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favorably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
– **Religion and/or Belief** (includes those with religion and /or belief and those with none)		
– **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)	No	
If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.		
Enter details here if applicable		

If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?	
Enter details here if applicable	
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A
Enter details here if applicable	
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk	
Was a full impact assessment required?	No
What is the level of impact?	Low

CONTENTS

1. INTRODUCTION

1.1 The purpose of this policy is to lay down the principles that must be observed by all who work within North Staffordshire Combined Healthcare and have access to person- identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. The Trust must ensure that it complies with Data Protection Law in its management and disclosure of person identifiable information, in addition to providing clear guidance for managers and staff. Additionally, all NHS organisations are required to comply with a number of standards that underpin the confidentiality of personal data within the Information Governance (IG) framework.

1.2 The IG framework allows organisations and individuals to ensure that personal and corporate information is managed legally, securely and efficiently in order to assist in the delivery of the best possible care.

1.3 The IG framework integrates previously separated but interrelated initiatives within a single transparent package which represents the Department of Health & Social Care Policy. There are similarities and overlaps between the core components of this framework. These core components currently include:-

- Freedom of Information Act 2000/Corporate Records Management including HSC 1999/053 For the Record;
- Data Protection Law Act 2018 & UK General Data Protection Regulation (UKGDPR);
- The Confidentiality NHS Code of Practice;
- Records Management NHS Code of Practice;
- Information Security Management;
- Information Quality Assurance;
- Caldicott Principles;

1.4 This policy details the rights of a “data subject” together with the responsibilities of the Trust. The Trust definition of a data subject is in accordance with Data Protection Law (DPA). Therefore, a data subject is defined as a living individual who is the (main) subject of personal data.

1.5 This policy details the “data controller”. The Trust definition of a data controller is in accordance with Data Protection Law (DPA). Therefore a data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

2. POLICY STATEMENT

In general any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. This duty of confidence is long established in common law. In addition, health professionals have ethical and professional duties of confidence.

The disclosure and use of confidential personal information needs to be both lawful and ethical. Whilst law and ethics in this area are largely in step, the law provides a minimum standard that does not always reflect the appropriate ethical standards that the government and the professional regulatory bodies require. For example, the Department of Health and the General Medical Council are in agreement that, whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for requiring that confidentiality obligations must continue to apply. Further, where the law is unclear, a NHS standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

Data subjects provide personal information for the employment/health records and have an expectation that their privacy will be maintained.

In this policy and supporting guidance 'personal information' applies to all such information about data subjects held in whatever form by the Trust.

It is neither practicable nor necessary to seek a person's specific consent every time information needs to be passed on for a particular purpose. Data subjects expect the NHS, often in conjunction with other agencies, to respond effectively to their needs. It can do so only if it has the necessary information. It is therefore essential that data subjects are fully informed of the uses to which information about them may be used. If the nature of the use of that information changes then the person to who the information relates must be informed and consent obtained before the information is passed on.

3. SUPPORTING GUIDANCE

The Duty of Confidence derives from the personal nature of the information recorded. It is unaffected by questions of who owns or holds particular records. Consequently, the following all have responsibilities for protecting information:-

- Everyone working for or with the NHS is bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within common law duty of confidence and Data Protection Law. It is also a requirement within the NHS Care Record Guarantee. This applies equally to those working on a voluntary basis or on a temporary placement such as students.

- Health Professionals have by virtue of professional regulation, an ethical duty of confidence which, when considering whether information should be passed on, includes special regard to the health of the patient and to his/her wishes.

- Other individuals or agencies to which information is passed legitimately may only use that information for specific purposes, possibly subject to particular conditions.

3.2 Human Rights Act 1998 (HRA98)

3.2.1 Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their records. Current understanding is that compliance with the Data Protection Law and the common law of confidentiality should satisfy Human Rights requirements. Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:-

- Pursue a legitimate aim;
- Be considered necessary in a democratic society; and
- Be proportionate to the need.

3.2.2 There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be

justified as being necessary to support legitimate aims and be proportionate to the need.

3.3 Data Protection Law

3.3.1 Data Protection Law relates to the rights and freedoms of living individuals. The Act gives individuals the right to access personal data held about them. Personal data relates to a living individual who can be identified from that data and includes any facts, opinion or any indication of intentions of the data controller about that individual. This includes personal data held in either electronic or manual systems.

3.3.2 NHS bodies that use personal information must register with the Information Commissioners Office (ICO). It is a criminal offence to hold or disclose information in breach of the registration requirement.

3.3.3 Any person who believes that the Trust has used or disclosed their personal information contrary to the requirements of the Law can apply to the Information Commissioner for an assessment to be undertaken as to whether any of the provisions of the Law have not been adhered to or to the Court for redress.

(See appendix 1 for the Data Protection principles)

3.4 Caldicott Report

Following a review of confidential patient information by the NHS, a series of recommendations for improvements to practice were made. NHS organisation must appoint a Caldicott Guardian to oversee the arrangement for the use and sharing of clinical information. The Trust's Caldicott Guardian is the Chief Medical Officer. The Trust must also comply with the principles set out in the Caldicott report.

(See appendix 2 for the Caldicott principles)

4. MANAGEMENT OF INFORMATION

4.1 The administration of personal information encompasses many elements. In all cases the use of personal information will be covered by a model referred to as HORUS (Holding, Obtaining, Recording, Using, and Sharing).

4.2 The Trust should ensure that data subjects are aware of the nature and source of any information kept about them, how it will be used and whom it may be disclosed to.

4.3 The Trust must inform data subjects about their rights under Data Protection Law, including their right to access the information kept about them.

4.4 Data subjects will be requested to confirm personal details kept on record that may be subject to change e.g. home address, GP etc.

4.5 The Trust will incorporate accuracy, consistency and validity checks into its associated systems.

5. RESPONSIBILITY OF STAFF TO MANAGE CONFIDENTIAL INFORMATON

5.1 All staff members must abide with the common law duty of confidentiality concerning the data and information used as part of their everyday work within the Trust. Under the Data Protection Act laws, members of staff must ensure that they have a lawful reason to use, disclose or share any personal or special category information with requestors. All staff must:

- Be aware of their personal responsibility for the protection of confidentiality and must abide by the policy and relevant legislations

- Ensure that details regarding patients/service users are not discussed in public or divulged to or in the presence of staff whose roles make such knowledge unnecessary. Staff must take particular are when talking in corridors, staff rooms or other public areas not to breach confidentiality

- Be aware that it is strictly forbidden to access a patient/service users record when there is no legitimate reason to do so. This for example could include searching for information about a relative, colleague, friend, neighbour, famous person, or even accessing their own record. Where necessary, the Trust will perform comprehensive system access audits and if unauthorised access/use is identified, this could lead to disciplinary action being taken which, in turn, could lead to a referral to staff professional bodies or dismissal

- Be aware that confidentiality covers non health data too, as, dependent on role, staff may have access to confidential information relating to other staff such as payroll, occupational health, or other employment matters

The following list summarises other key responsibilities:
Knowledge:

- Meet standards outlined in this and other related policies as well as in their terms of employment (or other engagement agreements)

- Be aware of and fully understand their legal and ethical obligations to keep personal information obtained through their work confidential

- Participate in induction, training and awareness raising sessions carried out to inform/update staff on confidentiality issues

- Be aware of the nominated staff within Information Governance Services and the Trust's Caldicott Guardian, whom they should liaise with regarding confidentiality issues

- Be aware of when information may be shared where the Trust is legally required to do so such as a Court Order

Putting Knowledge into Practice:

- Challenge and verify where necessary the identity of any person who is making a request for confidential information

- Report any actual or suspected breaches of confidentiality to their line manager and via the incident reporting system (Ulysses)

- Participate in audit/reviews of working practices to identify areas of improvement with regard to patient/service user confidentiality and to implement any measure identified

- Ensure data is recorded accurately, in accordance with the Trust policies on record keeping and is in line with the Records Management Code of Practice for Health and Social Care Records 2021

Respect for Service users:

- Make clear to patient/service users when information is recorded or when health records will be accessed – this may need to be no more than a simple phrase, such as “let me note that in your record” and should occur naturally as part of treating service users respectfully

- Check service users have seen the Trust Privacy Notices

- It is important for patient/service users to understand that carers and relatives may require certain information for them to provide effective care and support. They should be encouraged to disclose appropriate information to those they are close too who may be able to support them. It is important however to ensure that the patient/service user does not feel under pressure to allow the disclosure and that they can at any stage change their mind about this decision

- Where there is patient/service user agreement, then carers or relatives should be given sufficient information in a way that they can readily understand to help them provide care efficiently, this is to be documented within the health record

- Make clear to patient/service users when information is or may be disclosed to others. Examples may be in respect of:

    - A referral letter - “I am writing to the consultant to let them know about your medical history”
    - Other agencies – “I will tell Social Services about your housing needs to help them arrange accommodation for you”

- Explain clearly any reasons such as safeguarding where you may need to share information that has been shared by the service user if there is a risk of harm to them or others

- On occasion a clinician may be contacted by those close to the patient/service user about concerns regarding confidentiality. Confidentiality does **not** prevent clinicians from **listening** to carers /family about their experience and perspective of the individual’s presentation and health. Carers /family should be given the opportunity to discuss any difficulties, their experiences and observations. Receiving information from them is not breaching confidentiality

- Additionally, confidentiality does not prevent the clinician from providing certain information. These can include:

    - General information about mental health conditions
    - Contact details of lead health care professional etc.
    - Background information on medication and possible side effects
    - Contact details for local and national support organisations
    - Establishing communication strategies

- Where a patient/service user does not give permission for those closest to them to receive information about them, this should normally be respected – any reason to share information should be justified and documented on the patient/service user's record

- The patient/service user should be informed of the potential consequences of not involving carers/family in information about their care and that the clinical team retain a responsibility to support carers and families. This can include actions of continuing to maintain contact with the carer/family

- It is also necessary to consider whether the carer is a formal/employed carer (providing direct care via social services) or an informal carer such as a family member or friend

- Family (or friends) who are carers of an individual receiving services from the Trust are frequently anxious for information about the care being provided and may need some information to provide that care. Where a patient/service user lacks capacity it is likely to be essential that family and carers are involved in important decisions about the care

6. RESPONSIBILITY FOR DISCLOSING INFORMATION

6.1 The Caldicott Guardian ensures that the Trust is compliant in protecting the confidentiality of personal information and enabling appropriate information-sharing. The Caldicott Guardian will actively support work to facilitate and enable information sharing and advice on options for lawful and ethical processing of information as required.

6.2 Personal information may be disclosed on a 'need to know' basis, if the following circumstances apply:

- The use of the information can be justified e.g. confirmation of employment for mortgage application purposes.
- The information is required by statute or court order; or
- Passing on the information can be justified for other reasons, usually for the protection of the public or data subject.

6.3 The Trust is accountable for any decisions to disclose information. Such decisions should usually be taken by the health professional responsible for a patient's care or the manager holding the employee's personal information. If in doubt contact the Caldicott Guardian or Information Governance (IG) Team for advice.

6.4 Disclosure of personal information may also be decided on the advice of a nominated senior professional within the body or the directorate senior manager. Only the minimum identifiable information should be used.

6.5 Prevention of processing causing damage or distress – If an individual believes the Trust is processing personal data in a way that causes, or is likely to cause, substantial unwarranted damage or distress to them or to another, the Data Protection Law provides that the individual has the right to send a notice to the data controller requiring him, within a reasonable time, to stop the processing.

6.6 If a data subject wants information withheld from someone who might otherwise have received it in connection with their employment, then that data subject should be informed of any implications or other relevant factors.

Data subjects must make a request in writing if they do not want personal information disclosed which includes a description of:-

- The personal data;
- The purpose for which they are being processed; and
- Those to whom it may not be disclosed.

6.7 The data subject's wishes should be respected unless there are overriding considerations to the contrary. The reason for disclosing the information must be noted.

6.8 The data subject has a right to rectification if they feel that information recorded on their record is incorrect. This should be discussed with their line manager or clinician.

7. ANONYMISED INFORMATION

7.1 Where anonymised information would be sufficient for a particular purpose**,** identifiable information should be omitted. The Trust will endeavour to ensure that the recipient is unable to trace the data subject's identity. The fact that the information has been anonymised does not remove the legal obligations under the common law of confidentiality, Data Protection Law and the Human Rights Act.

7.2 Anonymising the information may not in all cases be sufficient to protect the data subject's identity: for example if they are from a professional group with only a small number of data subjects in the Trust.

8. CORPORATE AND STATISTICAL

8.1 The Freedom of Information Act 2000 (FOIA) is an element of the Government's commitment to greater openness in the public sector, a commitment which is fully supported by the Trust. The FOIA will progress this aim by helping to transform the culture of the public sector to one of greater openness. It enables members of the public access to substantial amounts of corporate information and documents therefore allowing the public to question the decisions of public authorities more closely, ensuring that the services we provide are efficiently and properly delivered.

8.2 Disclosure of information about performance and activity in the NHS is an important aspect of accountability and a means of fostering public awareness of how taxpayers' money is spent and the range of services provided.

8.3 Provided that the data subject is made aware that personal information may be used to prepare statistics only for management use, the aggregated information may be used or passed on for those purposes.

9. RIGHTS AND REDRESS

9.1 The unauthorised disclosure of data subject information by any member of staff or person in contact with the NHS is a serious matter and may result in the implementation of the performance management procedure or disciplinary action and possible legal action. In addition, health professionals may be subject to action by their regulatory bodies.

9.2 A duty of confidence forms part of the Trust's employment contract and terms and conditions of employment. All staff must be aware of the possible severe consequences of breaching confidence in relation to disclosure of personal information relating to data subjects.

9.3 **Patients** who feel their confidentiality has been breached should be encouraged to use the Trust's Listening and Responding PALS and Complaints policy (see policy 4.26).

9.4 **Employees** who feel their confidentiality has been breached have a duty to report this

immediately to their line manager and in addition, if they feel appropriate can take action in line with the Trusts Resolution and Grievances policy (see policy 3.02).

9.5 Data subjects have the right to refer their case direct to the Information Commissioner at the address below, to assess whether the requirements of Data Protection Law have been met.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow, Cheshire
SK9 5AF

Website: Information Commissioner's Office (ICO)
Email: casework@ico.org.uk
Telephone: 01625 545745

10. RISK & MONITORING COMPLIANCE WITH DOCUMENT

10.1 Risk management involves a two-stage approach to identifying both the points at which risk occurs in a system and solutions to reduce those risks. The first depends on reporting adverse incidents and near misses the second depends on the systems, structures and processes linked to the incident.

10.2 Monitoring of this policy will be through the incident reporting process (Ulysses) as any incidents of non-compliance with this policy (e.g. breach of confidentiality) must be reported via the Trust's electronic Incident reporting system

10.3 Failure to comply with the policy may result in the invocation of the performance management procedure or disciplinary action.

(Ref: Incident Reporting Policy No 5.01)

11. ACCESS TO DATA SUBJECTS INFORMATION

11.1 Data subjects have a legal right under Data Protection Law to access personal data about themselves which is held in either computerised or manual form by the Trust. This legal right is referred to as 'Subject Access Request' which enables an individual to review or to be provided with copies of information contained within any personal or occupational health record.

The data subject or their legal representative must make a request through the secure portal: Home Page - Portal (ams-sar.com)

A subject access request will be dealt with in line with the Trust's Subject Access Request policy No 7.02.

12. SECURITY OF PERSONAL INFORMATION

12.1 Ensuring the security and accuracy of data subject information is the responsibility of management and staff at all levels including:

- Arrangements for the storage and disposal of all data subject information (both manual and electronic) must protect confidentiality.

- Under Data Protection Law security measures must be in place to protect manual/paper and electronic information (see Information Security Policy No 7.03 and Records Management Policy 7.07).

- Care should be taken to ensure that unintentional breaches of confidentiality do not occur e.g. by leaving confidential information in publicly accessible areas or allowing conversations about sensitive personal information to be overheard.

- A non NHS agency or individual who is contracted to carry out NHS functions, the contract must draw attention to obligations on confidentiality. (see Information Security No 7.03)

- Those who work in the NHS must be aware that people may attempt to seek personal information by deception, for example, posing as a relative. If a member of staff is asked to provide non routine information by a person not known to them, they should make every effort to verify that the person has a right to the information before releasing it.

13. EXEMPTIONS RELATING TO PERSONAL DATA

13.1 Exemption Type: Duty of Confidentiality
Legislation: Common Law

Confidentiality is one of the factors that must be taken into account when deciding whether to disclose information without consent. A duty of confidence arises where information that is not generally available to the public (that is, genuinely confidential information) has been disclosed with the expectation that it will remain confidential. This expectation might result from the relationship between the parties. For example, the following relationships would generally carry with them a duty of confidence in relation to information disclosed.

- Medical (doctor and service user)
- Employment (employer and employee)
- Legal (solicitor and client)
- Financial (bank and customer)
- Caring (counsellor and client)

However, confidentiality should not always be assumed. For example a duty of confidence does not arise merely because a letter is marked confidential (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so does not have the “necessary quality of confidence”) or there may be other factors, such as the public interest, which mean than an obligation of confidence does not arise. In most cases where a duty of confidence does exist, it will usually be reasonable to withhold the information, unless the Trust has obtained consent to disclose it.

13.2 Exemption Type: Third Party Information
Legislation: DPA 2018, Schedule 2, Part 3 (16)

Information about third parties can be shared with other organisations as they are bound by the same confidentiality laws as this Trust. Where information about another individual is to be shared with an individual such as a service user or carer then careful consideration as to whether the information can be disclosed should take place.

This is known as balancing of the interests of the two individuals – does the right of access override the rights of the third party individual.

The Trust may find that in complying with requests for information, it will disclose information relating to an individual other than the data subject who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of information. The DPA 2018 sets out two circumstances in which the Trust is obliged to comply with the request in such circumstances, namely:

- Where the other individual has consented to the disclosure of the information; or
- Where it is reasonable in all the circumstances to comply with the request without the consent of the other individual

So, although the Trust may sometimes be able to disclose information about a third party, a decision needs to be made as to whether it is appropriate to do so in each case.

The Trust will make decisions about disclosing third party information on a case-by-case basis and not apply a blanket policy of withholding it. For the avoidance of doubt, the Trust cannot refuse to provide access to information about an individual simply because the information was obtained from a third-party source.

In line with DPA 2018 the Trust will not withhold the names of professionals who have complied or contributed to the health records or who have been involved in the care of the service user in their professional capacity. Special rules govern subject access to health, education and social work records. In practice these rules mean that relevant information about health, education or social work professionals (acting in their professional capacities) should usually be disclosed in response to a subject access request.

Considerations when making decision about disclosure should include:

- **Does the request require the disclosure of information that identifies a third party?**

The Trust will need to consider whether it is possible to comply with the request without revealing information that relates to and identifies third party individuals. In doing so, it should take into account the information to be disclose and any information that the Trust reasonably believes the person making the request may have, or may get hold of, that would identify the third party individual. As the DPA 2018 requires that the Trust provide information rather than documents, it may be possible to delete names or edit documents if the third party information does not form part of the requested information.

- **Has the third party individual consented?**

In practice, the clearest basis for justifying the disclosure of third party information in response to a request is that the third party has given their consent. It is therefore good practice to ask relevant third parties for consent to the disclosure of their personal data in response to a request. However, the Trust is not obliged to try to get consent and, in some circumstances, it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requestor anyway. Indeed, it may not always be appropriate to try to get consent for instances if to do so would inevitably involve a disclosure of personal data about the requestor to the third party. Consideration as to the reasonableness of seeking consent from third parties also needs to be considered.

- **Would it be reasonable in all the circumstances to disclose without consent?**

In practice, it may sometimes be difficult to get third party consent e.g. the third party might refuse consent or might be difficult to find. If so, the Trust must consider whether it is reasonable in all the circumstances to disclose the information about the third party anyway.

The DPA2018 provides a non-exhaustive list of factors to be taken into account when making this decision these include:-

- The type of information that would be disclosed
- Any duty of confidentiality owed to the other individual
- Any steps taken by the controller with a view to seeking the consent of the other individual
- Whether the other individual is capable of giving consent
- Any express refusal of consent by the other individual

Whether it is decided to disclose information about a third party in response to a SAR or to withhold it, the Trust will need to respond to the requestor.

If the third party has given their consent to disclosure information about them or if the Trust is satisfied that it is reasonable in all circumstances to disclose it without consent, the information should be provided in the same way as any other information provided in response to the SAR.

If consent of the third party has not been obtained and the Trust is not satisfied that it would be reasonable in all circumstances to disclose the third-party information, then it should be withheld.
However, the Trust is still obliged to communicate as much of the information requested as possible without disclosing the third party's individuals' identity. Depending on the circumstances it may be possible to provide some information, having edited or redacted it to remove information that would identify the third-party individual.

The Trust must be able to justify its decision to disclose or withhold information about a third party, so it is good practice to keep a record of any decisions made, and why. For example, it would be sensible to note why the Trust choose not to seek consent or why it was inappropriate to do so in the circumstances.

The decision to withhold third party information lies with the Trust and it is their responsibility to appropriately use this exemption balancing all the factors.

13.3 Exemption Type: Detrimental to Health (Serious Harm Test)
Legislation: GDPR Article 15 & DPA 2018 Schedule 3, Part 2 (2) & (5)

Separate provisions exist under DPA 2018 in relation to requests for health records in order to avoid disclosing material in inappropriate circumstances. The appropriate health professional must be consulted and give their written permission to release health information. They are responsible for making decisions to limit or deny access to health information. This is known as the "Serious Harm Test".

Under DPA 2018 the health professional is defined as someone who is currently, or was most recently responsible for diagnosis, care or treatment of the data subject in connection with the matters to which the data relates. Where this is more than one such health professional the health professional who is the most suitable to provide an opinion on the

questions should be contacted.

If the data subject has been discharged from services over three months ago (6 months for under the age of 13) then the health professional would not be contacted unless there were any specific concerns about disclosure. Where necessary guidance from another health professional who has the necessary experience and qualifications to provide an opinion on the requests could also be sought.

The serious harm test is met with respect to data concerning health if the disclosure of information using the data subjects right of access under GDPR to the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

When applying serious harm test the health professional should also document the decision making process and outcome within the health record. This should demonstrate that they have taken into account the following:

- Why they are of the opinion that to disclose the information would be likely to cause serious harm

- What considerations had been made around if certain parts of the information could be disclosed that would not meet the threshold for serious harm.

- What support could be offered to the data subject to aid disclosure and understanding of the information.

If the health professional still advises against disclosure as the serious harm test has been met, then the data subject would be informed of this decision and asked to reapply for this information in 3 months' time when the serious harm test can again be completed.

13.4 Exemption Type: Legal Proceedings
Exemption: DPA 2018, Schedule 2, Part 1, (5) (3) (a)

If a subject access request is received which would mean the disclosure of information would be likely to prejudice any legal proceedings or prospective legal proceedings, then this exemption can be used.

The decision in relation to the disclosure of this information would sit with the Information Governance as part of the normal subject access request process. Where applicable guidance would be sought from Legal Services.

13.5 Exemption Type: Legal Professional Privilege
Legislation: DPA 2018, Schedule 2, Part 4 (19)

If a subject access request is received which would mean the disclosure of information that is legally professional privilege being disclosed this exemption can be used.

Legally professional privilege is a set of rules of evidence that allows a party to litigation to withhold disclosure of certain categories of documents which are relevant to a dispute. There are two distinct aspects of Legal Professional Privilege:

- Litigation Privilege
- Advise Privilege

Litigation privilege covers all confidential communications made for the purpose of providing or obtaining legal advice about a proposed or contemplated litigation. There must be a real prospect or likelihood of litigation, rather than just a fear or possibility. It can be applied to a wide variety of information including advice, correspondence, notes, evidence or reports.

Advice privilege applies where no litigation is in progress or contemplated. It covers confidential communications between client and solicitor, made for the main purpose of seeking or giving legal advice. The adviser must have given advice in a legal context i.e. legal rights, liabilities, obligation or remedies. Advise about financial matters or strategic issues is not likely to be privileged.

The decision in relation to the disclosure of this information would sit with Information Governance as part of the normal subject access request process. Guidance from Legal Services to establish where Legal professional privilege can and cannot be applied to information being requested would always be sought when using this exemption.

13.6 Exemption Type: Management Forecasts
Legislation: DPA 2018, Schedule 2, Part 4 (22)

If a subject access request is received which would mean the disclosure of information relating to management forecasts or management planning in relation to a business or other activity to the extent that the disclosure would be likely to prejudice the conduct of business or activity, then this exemption can be used.

The decision in relation to the disclosure of this information would sit with Information Governance as part of the normal subject access request process.

13.7 Exemption Type: Negotiations
Legislation: DPA 2018, Schedule 2, Part 4 (23)

If a subject access request is received which would mean the disclosure of information relating to records of the intention of the Trust in relation to any negotiations within the data subject to the extent that the disclosure would be likely to prejudice those negotiations then this exemption can be used.

This exemption would be applicable in areas such as negotiations about pay and conditions or prospects with an employee. This can also be used in the wider context in terms of negotiations with consultants and/or trade unions.

The decision in relation to the disclosure of this information would sit with Information Governance as part of the normal subject access request process.

13.8 Exemption Type: Confidential References
Legislation: DPA 2018, Schedule 2, Part 4 (24)

This exemption allows the Trust to refuse to disclose a confidential employment reference to an employee or former employee if they request access to it. This exemption covers both those confidential references given by the Trust or received by the Trust. When dealing with requests for access to references it is fundamental to ensure that the level of confidence attached to the reference is considered and if sharing of the reference could lead to an actionable breach under common law.

In most cases, references received by the Trust should be considered confidential and

consent from the third party sought if appropriate before disclosure. References given by the Trust in most instances will be a factual only reference produced by Human Resources so would not be considered confidential. The decision in relation to the disclosure of references would sit with Information Governance as part of the normal subject access request process.

The above list focusses on those exemptions which are commonly used by this Trust when dealing with subject access requests. This list of exemptions under GDPR and DPA 2018 is not exhaustive and further details can be found on the Information Commissioners Office website www.ico.org.uk

14. CO-ORDINATING INFORMATION WITH EXTERNAL SERVICES

14.1 Access to personal identifiable information should be restricted to those who have a justifiable need to know in order to effectively carry out their jobs. The Caldicott Principles underpin the approach taken by the Trust when requested to share information with other NHS organisations and non NHS organisations for example Social Services. Sharing information, current or proposed, should be tested against the Caldicott Principles (see appendix A).

14.2 Trust protocols provide a robust framework for staff when sharing personal identifiable information. The purpose(s) for which information is required by different organisations will clearly differ and each needs to be sensitive to the particular requirements of others in respect of confidentiality.

14.3 The data subject needs to be aware that some information sharing for direct care will be necessary and this must be discussed with the individual as part of the care planning process.

14.4 If the data subject raises any objections to the passing of information to other sources, the possible consequences must be explained and an assurance given that other sources would receive only information which they really need to know. However, the data subject's ultimate decision must be respected unless there are overriding considerations to the contrary: for example, in some cases involving a history of violence, or where an elderly frail person shows signs of non-accidental injury, it may be justifiable to pass information to another agency without the individual's agreement.

14.5 When creating inter-agency registers or pooling information to assist joint commissioning of services, NHS (and other) bodies should ensure that patients know in general terms what is being done and to whom information may be passed.

14.6 Any new services that are implemented a Data Protection Impact Assessment (DPIA) must be completed to demonstrate how the processing of data will be managed, shared and safeguarded. This will identify any associated risks.

15. PARTICULAR RESTRICTIONS ON PASSING ON INFORMATION

NHS bodies or those carrying out NHS functions must not allow personal details of data subjects (most obviously names and addresses of named individuals) to be passed on or sold for fundraising or commercial marketing purposes.

16. DISCLOSURE OF INFORMATION FOR OTHER PURPOSES OR AS A LEGAL REQUIREMENT

16.1 There are statutory powers to order:

- The disclosure of documents before and during proceedings for personal injury or death.

- The production of information following an application to the court and to the applicants, legal, medical and professional advisors. Such orders should specify clearly what information is required and by whom. If any aspect is unclear, clarification and/or legal advice should be sought without delay. The manager responsible for the information relating to the data subject should be consulted about the disclosure, in case disclosure may result in a risk to the data subject. If there is a risk, legal advice should be sought on the possibility of seeking an amendment to the order.

- Where an order requires information about a data subject who has not instigated a court action, that data subject should be notified immediately in case the individual may wish to seek advice.

At the data subject's request, information relevant to legal proceedings may be released, usually to the individual's legal adviser. This information should also be passed to solicitors acting for the Trust where the action involves the Trust. Ref: Subject Access Request Policy No 7.02.

16.2 Relatives, friends and carers, if data subjects agree can be kept up-to-date with the progress of treatment. With the data subjects consent, the significant role of carers may need to be recognised in the type of information provided. If the data subject has not given their consent then information should not be passed to relatives etc.

17. DISCLOSURE OF INFORMATION TO PROTECT THE PUBLIC

17.1 It may sometimes be justifiable to pass on data subject information without consent or statutory authority. Most commonly these involve the prevention of serious crime, but can extend to other dangers to the general public, such as public health risk or violence. Essential information may need to be shared with other agencies.

17.2 Each case must be considered on its merits, the main criterion being whether the release of information to protect the public should prevail over the duty of confidence to the data subject. The possible consequences for the data subject must always be considered.

17.3 Decisions will sometimes be finely balanced and may concern matters on which NHS staff find it difficult to make a judgement. In such cases legal or other specialist advice e.g. Caldicott Guardian should be sought. It is important not to confuse 'the public interest' with what may be 'of interest' to the public.

18. TACKLING SERIOUS CRIME

18.1 Passing on information to help tackle serious crime may be justified in accordance with the Crime and Disorder Act 1998.

Whilst the police have no general right of access to personal information there are a number of statutes which require disclosure to them and some that permit disclosure. These have the effect of making disclosure to them and some that permit disclosure a legitimate function in the circumstances they cover.

In the absence of a requirement to disclose there must be either explicit consent of the data subject or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the Courts. Where disclosure is justified it should be limited to the minimum necessary to meet the need and the data subject should be informed of the disclosure **unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk.**

18.2 Disclosure must be justified on the grounds that the public interest outweighs the common law duty of confidentiality and the principles of the Human Rights Act 1998 (HRA98).

Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with Data Protection Law and the common law of confidentiality should satisfy Human Rights requirements.

Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:

- Pursue a legitimate aim;
- Be considered necessary in a democratic society; and
- Be proportionate to the need.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need. Ref: Subject Access Request Policy No 7.02.

19. TEACHING AND RESEARCH

19.1 Advice to data subjects about the use of personal information must emphasis:

- The importance of teaching and research to the maintenance and improvement of care within the NHS, inter-agency care and public health generally;

- That such information, anonymised or aggregated wherever possible, may sometimes be used for teaching and research (and that universities or other bodies carrying out approved research are required to treat it in confidence and must not use if for other purposes);

- That any research proposals involving access to patient records require regulatory approvals including a favourable ethics opinion from a Research Ethics Committee, who must be satisfied that:

    - Arrangements to safeguard confidentiality are satisfactory;
    - Any additional conditions relating to the use of information that the Research Ethics Committee thinks are necessary are met;

- Any application to use **identifiable** patient information is fully justified: for example, because this is essential to a study of major importance to public health. **If not, approval to proceed should not be given;**

- That their specific consent will be sought to any activity relating to teaching or research that would involve them personally. Individuals may at any time state that they do not wish to be contacted for involvement in such activity and this must be formally recorded

so that they are not contacted.

- That any publicised research findings will not identify them without their specific consent.

20. TRAINING REQUIREMENT

20.1 Confidentiality training is included within the annual Data Security Awareness e-learning training tool and will be monitored through the Trust Mandatory training and the Personal Review process.

21. COMMUNICATION WITH THE MEDIA

21.1 The maintenance of good relations with the press and broadcasting organisations is important. The Trust will ensure that there is someone with suitable experience and level of responsibility available or contactable at all times to answer enquiries.

21.2 If the media interest relates to a data subject, then the individual's valid consent must be obtained before release of information. If the person is incapable of providing valid consent then the consent of the nearest relative should be sought.

21.3 Neither the Trust nor anyone who works in the Trust should confirm that any individual is a data subject or divulge any information about them without the person to which the information refers consenting to its release.

21.4 Subject to the necessary consent being given, a brief indication of the patient's progress or the employee's job title and work base may be given in response to media enquiry if authorised by the Senior Manager.

21.5 As referred to above, other than straightforward data subject enquiries, media requests for information should be referred to the Communications Manager, Corporate Services or the Caldicott Guardian.

21.6 Where the data subject is unable to take a decision, the provision of basic information may sometimes be judged to be in their best interests (e.g. correcting misleading or damaging speculation).

21.7 If a data subject has invited the media to report their case, the Trust may comment in public but should confine itself to factual information or the correction of any misleading assertion or published comment. The duty of confidence to the data subject still applies. If in doubt, legal advice should be sought.

22. EQUALITY IMPACT ASSESSMENT

An equality impact assessment has been undertaken for this policy with no potential or adverse impact identified.

23. REFERENCES & OTHER SOURCES OF INFORMATION

- Risk Management Policy No 4.18a
- Incident Reporting Policy No 5.01
- Serious Incident Policy No. 5.32

- Subject Access Request Policy No 7.02
- One Staffordshire Information Sharing Protocol Policy No 7.05
- Information Governance Policy No 7.08
- Information Security Policy No 7.03
- Records Management Policy 7.07
- Caldicott Guardian caldicott guardian - Search - GOV.UK (www.gov.uk)
- NHS Confidentiality Code of Practice Confidentiality: NHS Code of Practice - GOV.UK (www.gov.uk)
- Record Management: NHS Code of Practice Records management: code of practice for health and social care - GOV.UK (www.gov.uk)
- Information Security Management: NHS Code of Information Security Management: NHS Code of Practice - GOV.UK (www.gov.uk)
- Cyber Security Codes of Practice Cyber security codes of practice - GOV.UK (www.gov.uk)
- NHS Shared Care Records NHS England » Shared care records

APPENDIX 1

DATA PROTECTION; PRINCIPLES OF DATA PROCESSING

Principle 1	Personal data shall be processed lawfully, fairly and in a transparent manner;
Principle 2	Collected for specific; explicit and legitimate purposes;
Principle 3	Personal data shall be adequate, relevant and limited to what is necessary;
Principle 4	Personal data shall be accurate and, where necessary, kept up to date;
Principle 5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
Principle 6	Personal data shall be processed in an appropriate manner to maintain security;
Principle 7	The Data Controller is accountable and responsible and able to demonstrate compliance with all the above principles.

APPENDIX 2

THE CALDICOTT GUARDIAN: PRINCIPLES

Principle 1	Justify the purpose(s) for using confidential information;
Principle 2	Do not use person identifiable information unless it is absolutely necessary;
Principle 3	Use the minimum necessary person-identifiable information;
Principle 4	Access to person-identifiable information should be on a strict need to know basis;
Principle 5	Everyone with access to person-identifiable information should be aware of their responsibilities;
Principle 6	Understand and comply with the law;
Principle 7	The duty to share information can be as important as the duty to protect person-identifiable confidentiality;
Principle 8	Inform individuals about how their confidential information is used.

APPENDIX 3
GUIDANCE FOR SENDING OR RECEIVING CONFIDENTIAL INFORMATION

Post or Courier

- Use appropriate stationery such as secure document bags where necessary
- Check that the recipient's name and address are correctly typed or clearly written in indelible ink
- If using a window envelope ensure that the name and address are clearly visible and that no other information is visible
- The envelope should be labeled or stamped accordingly e.g. confidential, addressee only etc.
- Ensure that the only documents placed in the envelope is for that recipient and that nothing else has accidently become attached or included
- If confidential information is being sent through the Trust internal post then ensure that the secure green document bags are used and that his is labelled clear for the intended recipient with the correct Department and Location and the bag must be sealed

E-mail

- Do not send confidential emails to external email addresses without encryption (just type [SECURE] at the beginning of the subject link.
- If you are pressurised to send without encryption – please contact the IG Team
- Always double check that you have typed in the correct email address, if you are using the outlook address book ensure that you have the correct person as they may be several staff with the same name
- If you are sending an email to multiple recipients outside of the organisation, always us 'BCC' so that their individual email address cannot be seen by the other recipients

Receiving Confidential Information

- Ensure that you provide your full contact details e.g. correct email address or full name and postal address
- If confidential ask the sender to mark the envelope as such and address F.A.O.
- If post is marked as 'Addressee Only' then it should not be opened by any other person
- If post is marked as confidential it could be opened by another member of the team in that persons absence
- Once confidential information is received then is should be processed accordingly and the document to be filed or destroyed as appropriate

Telephone/MS Team Calls

- Do not make calls in an environment where you could be overheard if confidential information is being discussed
- When staff are making calls in a shared area be mindful what you discuss with others as the caller may overhear background conversations
- When receiving a call to discuss confidential information you should check to confirm you are speaking to the correct person

Doc level: Trust
Code ref: 7.03

7.03 Information Security Policy

Lead executive	Director of Partnership, Strategy & Digital
Authors details	Head of Information Governance Deputy Chief Information Officer

Type of document	Policy
Target audience	North Staffordshire Combined Healthcare NHS Trust workforce
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet legal responsibilities in relation to Information Security.

Approval meeting	Senior Digital Team including Caldicott Guardian & Senior Information Risk Officer.	Meeting date	20th March 2024
Ratification date		Review date	30th April 2027

Trust documents to be read in conjunction with	
Document code	Document name
3.01	Disciplinary Procedure
4.18a & b	Risk Management Policy and Strategy
7.01	Confidentiality of Employee and Patient Records
7.02	Subject Access Request Policy
7.07	Records Management Policy
7.14	Safe Haven Policy
7.22	Registration Authority Policy

Document change history		Version	Date
What is different?	– Policy has been rewritten to simplify and make more user friendly for staff – The following policies have been incorporated in this policy and can be withdrawn on approval of this policy: • Pol 7.16 IT Assets • Pol 7.21 Information Risk • Pol 7.19 Mobile Information Handling	0.1 0.2	29.09.2022 25.10.2022
	– Bring Your Own Device section added	0.3	08.03.2024
Appendices / electronic forms	– Definitions appendix added – Version control appendix added		
What is the impact of change?	– Ensuring that staff are aware of their responsibilities and the important of keeping all Trust assets safe and secure		

Training requirements	All staff are mandated to complete the online Data Security Awareness national training tool annually as well as other identified specialist training requirements dependent upon job role.

Document consultation

Directorates	Partnerships, Strategy & Digital
Corporate services	Corporate Governance
External agencies	

Financial resource implications	No

External references
1. Data Protection Act 2018 2. UK General Data Protection Regulations (UK GDPR) 3. ISO27001 Information Security Standard

Monitoring compliance with the processes outlined within this document	Any breaches to this policy will be recorded within the Trust's incident reporting system and will be investigated accordingly. This policy will be monitored and updated accordingly by the Data Protection Governance Steering Group

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favourably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	

– **Religion and/or Belief** (includes those with religion and /or belief and those with none) – **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)	No	

If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.	
Not Applicable	
If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?	
Not Applicable	
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A
Not Applicable	
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk	
Was a full impact assessment required?	No
What is the level of impact	Low

Contents

1. Introduction

The aim of information security is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust.

North Staffordshire Combined Healthcare NHS Trust is committed to achieving the following Information Security and IG objectives:

- Establish and maintain policies for the effective and secure management of its information assets and resources
- Undertake or commission annual assessments and audits of its information and IT security arrangements
- Promote effective confidentiality and security practice to its staff through policies, procedures and training
- Establish and maintain incident reporting procedures and will monitor and investigate all reported instance of actual or potential breaches of information, confidentiality and security.

Information security is everyone's responsibility and this policy sets out to ensure that information is protected from threats and confidence is maintained that our data is accurate and of good quality, through the use of technical developments and organisational management procedures.

2. Scope

This policy applies to the whole workforce at North Staffordshire Combined Healthcare NHS Trust including full-time and part-time staff, students, trainees, seconded, volunteers, contracted third parties and any other persons undertaking duties on behalf of the Trust.

It applies to all forms of information processed by the Trust and covers all business functions, information systems, networks, hardware, software, applications, mobile devices physical environments and relevant people who support those business functions.

Any breaches of this policy will be subject to the existing Trust Disciplinary Policy 3.01.

This policy will be referred to when dealing with other agencies in order to give clear guidance on the Trust's approach to information security but it does not represent the policies, procedures or guidelines of other agencies.

3. Definitions

Owing to the breadth and level of technical complexity of this policy, all relevant definitions may be found at Appendix 1.

4. Information Security Regulations, Standards and Principles

Information Security is defined as the preservation of confidentiality, integrity and availability of information:

Confidentiality: Confidentiality can be defined as having another's trust or confidence or be entrusted with secret or private affairs. We do this with the health records we hold. In addition to the specific rules, we all have to abide with the Common Law Principle of Confidentiality.

Integrity: Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire life cycle. Data must not be subject to unauthorised change, whether in transit, at rest or in use. Steps must be taken to ensure that unauthorised people cannot alter the data.

Availability: Availability of information refers to ensuring that authorised parties are able to access the information when required. Information is only of value if the right people can access it at the right times.

5. Statutory Obligations

The General Data Protection Regulation (GDPR) was introduced in May 2018 and enhances the rules and obligations on those persons and organisations that process personal and special category data. Amongst those obligations are heightened information security standards. The Data Protection Act 2018 enacted GDPR into UK Law and we now refer to UKGDPR.

6. National Data Guardian Security Standards

The Trust is required to complete an online self-assessment annually; The Data Security and Protection Toolkit. This allows the Trust to measure performance against the National Data Guardian's 10 Data Security Standards.

7. Information Risk Management

Information risk is inherent in all activities and everyone working for or on behalf of the Trust continuously manages information risk.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions.

It should be noted that this policy complements and does not supersede the Trusts Risk Management Policy and Strategy documents.

7.1 Information Risk Management Roles

To manage information risks, the following key roles have been identified

- Senior Information Risk Owner (SIRO)

- Chief Information Officer/Deputy Chief Information Officer
- Head of Information Governance/Data Protection Officer
- Information Asset Owner (IAO)
- Information Asset Administrator (IAA)

8. Information Asset Management

8.1 Information Assets

Major information assets are those that are central to the efficient running of business critical functions for the Trust, ie patient, finance and personnel management processes.

There are four main categories of information assets:

Information, Software and Hardware

Databases, system documentation and procedures, archive media, application programs, systems, development tools and utilities including:

- Digital or hard copy patient health records (including those concerning all specialties and GP medical records)
- Digital or hard copy administrative information (including, for example, HR, estates, corporate planning, supplies ordering, financial and accounting records)
- Digital or printed x-rays, photographs, slides and imaging records, outputs and images
- Digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disk drives, removable memory sticks, mobile phones and other internal and external media compatible with NHS information systems)
- Computerised records, including those that are processed in networked, mobile or standalone systems
- Email, text and other message types such as eFax solutions

Where a data protection impact assessment (DPIA) identifies that an asset is of sufficient criticality to the Trust, it may require that dedicated staff are appointed to assist in its management, e.g. an information asset owner (IAO) and whether additional business continuity (BCP) or disaster recovery (DR) plans are required (done in conjunction with Staffordshire & Shropshire Health Informatics Service (SSHIS)).

SSHIS maintain an IT hardware and software register which details assets based on their location. Staff should not move any IT equipment without notifying SSHIS.

The procedure for purchasing hardware and software can be found on the Trust intranet. This procedure must be followed to ensure that everything is paid for and therefore legal. The introduction/installation and/use of unauthorised hardware/software on Trust sites or Trust owned assets is a disciplinary offence.

Object and source code for system software will be securely stored when not in use by the developer. Developers must not have access to modify program files that actually run in production. Changes made by developers must be implemented into production by technical staff. Unless access is routed through an application interface, no developer will have more than read access to production data.

Furthermore, any changes to production applications must follow the change management process. Developers must at least perform unit testing. Final testing must be performed by the clinical systems team or the target user population.

SSHIS maintain a Definitive Software Library (DSL) that contains the authorised version of all software in use. Only authorised software will be accepted into the DSL. Access to the library is strictly controlled.

SSHIS will carry out a reconciliation of software licenses at not less than 12 monthly intervals to verify that the number of licenses held matches the number of equivalent software installations. The results of the software audit will be made available to Trust managers and all anomalies investigated and corrected.

Other than access to electronic mail via Outlook Web Access (https://mail.northstaffs.nhs.uk), or access using secure authentication (Remote Access Service), staff must not process or store Trust information on their own equipment.

Physical

This includes infrastructure, equipment, furniture and accommodation used for data processing. No physical asset that is capable of holding information may be purchased outside of Trust procurement procedures.

Utilities and Services

This includes computing and communications, heating, lighting, power, air conditioning used for processing data. Local responsibility for the asset may be delegated to the Departmental Manager working in the relevant service area.

People

This includes people and their qualifications, skills and experience in the use of information systems. Each owner is responsible for ensuring that new and existing people are correctly skilled to perform their duties.

8.2 Disposal of IT Hardware and Related Media

Many IT components are highly toxic, releasing arsenic, bromine, cadmium, lead, mercury and other chemicals into the environment if not treated properly before being dumped in landfill sites.

The Waste Electrical and Electronic Equipment Directive (WEEE Directive) aims to minimise the impact of electrical and electronic goods on the environment, by increasing re-use and recycling and reducing the amount going to landfill. The UK Regulations implementing the WEEE Directive came into force in January 2007. All IT equipment must be disposed of in accordance with this Directive.

To minimise the risk of data being lost all magnetic media including hard drives will be physically destroyed.

For the purposes of this policy, IT hardware and related media **includes**:

- The personal computer (also referred to as CPU, base unit / tower / desktop / laptop etc.)
- Monitor, printer, keyboard, mouse and other peripheral devices

- Magnetic media such as hard disk drives, CDs, DVDs, tapes, USB Memory Sticks
- Photocopiers
- Projectors
- Jayex boards
- Telephone equipment

SSHIS will arrange for the safe/secure disposal of all IT hardware and related media. Any costs associated with this process are to be paid for by the budget holder responsible for the equipment being disposed of.

8.3 Information Classification

8.3.1 Owners and Production Information

All electronic information managed by the Trust must have an Information Asset Owner. Production information is information routinely used to accomplish business objectives. Owners should be Director level and responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. There are designated members of the Trust management team who act on their behalf, and who supervise the ways in which certain types of information are used and protected.

- **RESTRICTED**—this classification applies to the most sensitive business information that is intended for use strictly within the Trust. Its unauthorised disclosure could seriously and adversely impact the Trust, its service users, its business partners, and its suppliers

- **CONFIDENTIAL**—this classification applies to less-sensitive business information that is intended for use within Trust. Its unauthorised disclosure could adversely impact the Trust or its service users, suppliers, business partners, or employees

- **PUBLIC**—this classification applies to information which has been approved by the Trust management for release to the public. By definition, there is no such thing as unauthorised disclosure of this information and it may be disseminated without potential harm

9. Information Security Incident Management

An information security incident is defined as an event, which has resulted, or could result in:

- The disclosure of confidential information to any unauthorised individual. This includes manual and computerised information
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact, for example:
    - embarrassment to a patient
    - embarrassment to the NHS
    - legal obligation or penalty
    - disruption of activities
    - financial loss to the Trust

- threat to personal safety or privacy

Some examples of security incidents are:

- An IT system becoming infected with a computer virus
- A user's password becoming known to other persons and used to access systems without authorisation
- Unauthorised access to confidential information/data, i.e. smartcard left in machine to be used by another member of staff
- Theft of computer hardware or health records containing patient-identifiable information

All Information Security incidents and near misses should be reported on the Trust Incident Reporting System (Safeguard).

There are occasions where confidential information is sent to the Trust in error by other organisations. These are known as **non-incidents-confidential documents received in error**. Whilst these are not strictly speaking an incident to be added to Trust Incident Reporting System (Safeguard) as they are not our breach, we have taken the decision to monitor them.

Should we then be questioned by any authority at a later date we can show due care by behaving responsibly and notifying the senders and the Information Security Department involved.

If you receive any such information, you should notify the IG staff by email, giving the date, person/organisation and your response will be sufficient for our register.

Do not forward the mail you have received as this may result in a further breach (by our Trust).

9.1 Information Governance (IG) Investigations

GDPR Article 33 compels a Controller to report, without undue delay and, where feasible, not later than 72 hours after having become aware of it, any breaches of personal data to the supervisory authority. For the Trust, this reporting is to the ICO, via the NHS Digital (NHSD) Data Security and Protection (DSP) Toolkit.

NHSD will issue the criteria and scoring scales to determine whether an incident shall be reported or can be managed locally. The DPO will issue processes to ensure that all reported incidents are investigated and reported internally to the relevant committee and, where necessary, to the ICO.

Where an IG incident appears to require reporting to the ICO, the DPO is to consult with the SIRO and the Caldicott Guardian before making their report. A consensus of these three officers will give balance and determine if the matter should be reported.

All IG investigations and information security incidents (including cyber) reporting will be in line with the Trust's overall incident reporting processes, following the procedure outlined in the Trust's incident reporting policy.

Where IG investigations tend to relate to disciplinary matters, then all evidence is to be gathered and presented in a manner where it meets the evidential requirements of the HR investigation policy.

9.2 Systems Audits

At the discretion of the DPO, IG staff will be granted access to all or any asset to undertake audits into its use. Operational managers may request audits into any specific allegation of misuse of an information asset but IG staff are not able to run routine ongoing audits where no specific evidence exists to justify that course of action; the DPO will have the final decision in all such matters.

9.3 IT Forensic Readiness

The Trust is required to have effective availability of reliable digital evidence gathered from its information assets to allow consistent, rapid investigation of major events or incidents with minimum disruption to Trust business. This is known as IT Forensic Readiness Planning.

IG staff will use the DPIA process to identify the capability of a given asset to be able to provide digital evidence in this manner.

9.4 Seizing and Securing Computer Systems for Evidence

When it is anticipated that computer systems are likely to be required as evidence to support disciplinary or criminal investigations, then IG staff are to be approached for advice.

In all cases, the National Police Chiefs' Council's *Good Practice Guide for Digital Evidence (ACPO)* is to be followed. The latest version dated March 2012 was issued under their old name of the Association of Chief Police Officers. Under no circumstances, are staff to attempt to examine computers that are suspected to be involved in criminal activity. This includes turning on and logging on to the computer involved. Such activity may render any evidence unusable.

9.5 Business Continuity Planning and Disaster Recovery

Business Continuity Planning (BCP) and Disaster Recovery (DR) for information assets are intended to provide staff with access to business critical clinical and administrative systems at an agreed reduced level during unscheduled periods of disruption.

Business Continuity Planning may be described as the actions taken by ordinary users of information assets to respond to an unplanned disruption with a view to them being able to continue to offer a service to our patients and service users.

BCP is largely with the clinical areas although supported by digital. This is system specific – some areas have digital solutions whilst other have manual processes.

The digital team work with SSHIS to define the Recovery Time Objectives (RTO's) and Recovery Point Objectives (RPO's) to meet the Trust requirements.

DR may be described as the actions taken to SSHIS and relevant staff members to restore an information asset within an agreed timescale in case of an unplanned disruption.

DR is largely done by SSHIS through technologies agreed at board level.

9.6 BCP Testing

SSHIS is a strategic partner and works with the Trust to ensure that the BCPs are adequately tested.

SSHIS hold the Trust DR plans and documentation specific to the systems and service provided to the Trust. These are evidenced as part of the toolkit.

10. Network Structure, Configuration and Security

10.1 Overview

Network Security is vital in protecting Trust data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats.

10.2 Network Equipment

Only Trust approved devices should be connected to the network and under no circumstances should personal equipment or devices be connected to the Trust network infrastructure. This excludes personal devices being connected to Trust supplied guest Wi-Fi or another approved network.

10.3 Physical and Environmental Security

Physical and environmental countermeasures are to be adopted to minimise the risk of a breach of security to all network resources. All Trust IT assets are to be kept under lock and key when they, or the building that they are stored in, are left unattended.

This includes, when a computer is left unattended in a location where members of the public have access, e.g. consulting rooms. It is also the responsibility of each member of staff to ensure that any computer they are using is not exposed to any excessive likelihood of theft. Where such a risk exists then they are to notify their line manager; the advice of IG staff may be sought. In some cases, the use of additional security devices, e.g. security cages or cables, may be necessary.

Data Centre Access

Access to the data centre must be physically restricted

Facility Access

All network equipment (routers, switches etc) and servers located in corporate offices and in all facilities must be secured when no Trust staff or authorised contractors are present.

Fire Suppression Systems

All Server Rooms and other key ICT installations are to be risk managed to decide whether or not they have fire suppression systems installed. Where installed, the fire suppression systems are to meet, and be maintained, in accordance with the appropriate legislation.

Uninterruptible Power Supplies

Uninterruptible Power Supplies (UPS) are devices that provide battery backup when the electrical power fails or drops to an unacceptable voltage level and give protection against power surges or spikes. UPS devices provide power for a few minutes; enough to power down the computer in an orderly manner, or maintain services during brief power disruptions. They are not designed to be an alternative source of power. UPS devices are to be fitted to servers and other key network devices.

Air Conditioning

Air conditioning systems may be fitted to server and communications rooms to ensure that the temperature and humidity levels in these rooms allow the computers to work at optimum levels. The requirement for air conditioning is to be risk managed based upon the individual circumstances of each location.

Physical Location of Server Rooms and Key ICT Assets

When new server rooms or other key network assets are being planned, due consideration is to be given to minimise the risk to damage through theft, fire, flood or other natural disaster. Likewise, consideration is to be given minimising the risk from accidental or malicious damage, e.g. vehicle collision or vandalism. The financial costs of these measures are lower when incorporated into new builds when compared against upgrading existing facilities. All existing facilities are to be subject to ongoing reviews to ensure that any risks are minimised.

Standby Generators

Where appropriate, consideration should be given to providing power to essential network equipment from standby generators in order to mitigate risk of damage to data and equipment through ungraceful shutdowns.

Network Cabling

Cables are essential to the transmission of information assets and to the provision of information services, but they expose risks to the availability and confidentiality of information assets and also to continuity of business operations. These risks may arise from damage to, interception or interference with these cables. Furthermore, personnel with access to these cables may accidentally cause damage.

Consideration should be given to protecting information assets via cables against unauthorised access, use, damage or destruction by implementing appropriate measures such as secure routing of cable, armoured conduits and placing the cables underground where feasible. Cables should be subject to inspections at regular intervals to ensure that no unauthorised device is connected to the cables. Access control procedures and measures for access to cable rooms and patch panels should be established.

Social Engineering

Criminals that want to steal data may use tricks to manipulate you to give them access to valuable information such as health records, patient data or IT system information - this is called social engineering.

There are many ways a social engineer may try to get information from you – here are some examples:

- Call you and pretend to be a colleague or someone from your IT helpdesk
- Ask you to hold a door open for them
- Pretend to be a ‘friend’ on social media

Often a social engineer will spend weeks getting to know an organisation before trying to get physical entry or making a phone call – they may find a phone list or organisational chart and use social networking sites like LinkedIn or Facebook.

What you can do to stop social engineering

- Always be vigilant at work – using the phone, receiving unsolicited emails, using social media or walking around your office – consider what information could be valuable to a social engineer
- Never reveal your login details to anyone – SSHIS and digital colleagues will never ask you for your login details
- Challenge suspicious behaviour and ask for ID – only if it's safe to do so
- Take extra care when using websites - if you get a message that you are about to use an untrusted website, it could be a fake phishing site – these can look extremely authentic and could trick you into giving away personal information
- Red padlocks mean beware - if you see a red padlock or warning message, your connection may not be private – again take care
- Think about what information you share on social media about your work – if a criminal can find posts so can your employer which could result in disciplinary action

Clear Desk

NHS employees and contractors are required to ensure that all confidential information is secure within their work area. To ensure this level of confidentiality, the following measures are to be adopted:

- Confidential information, this may include diaries, notes, post its etc. must be secured when the desk is vacated – this includes meeting rooms
- Information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day
- Drawers containing confidential information must be kept locked when not in use or when not attended
- The keys used for access to the drawer must be kept secure at all times and access can be gained if necessary by a senior member of staff
- Any confidential information such as records that may need to be used by other members of staff must be place in the relevant filing cabinet and locked
- Printouts containing confidential information should be immediately removed from the printer
- All paper confidential waste must be disposed of separately to 'standard' waste and must be stored securely in an office, ward, clinic etc until it is disposed of.
- Confidential waste must be placed in appropriately marked repository bins, bags or sacks. All confidential waste must be disposed of (incinerated or shredded under supervision.
- Whiteboards containing confidential information should be erased or concealed with a shutter and lock to prevent their contents being viewed.
- Treat mass storage devices such as CDROM, DVD or USB drives as confidential and secure them in a locked drawer
- Ensure computer workstations are locked or logged off when left unattended

- Reception areas should be kept as clear as possible to avoid records being within reach/sight of any visitors to the Trust and any visitor, appointment or message books should be stored in a locked area when not in use

Off-Site

- Portable electronic equipment must be kept in the possession of a Trust employee during transportation. If such equipment is lost or stolen, the matter must be reported to your line manager and SSHIS
- Equipment or paper files should be kept out of sight, locked away and not be left unattended
- Where a courier service is used to transport packages containing sensitive information, tamper proof packaging will be used. Courier firms should guarantee the safe arrival of parcels and the confidentiality of any contained information
- Portable electronic equipment must have encrypted protection against unauthorised use. Passwords for example on boot-up (when a computer is switched on), should be incorporated
- Where the Trust has supplied any form of data device, only appropriate members of staff are authorised to access it. Any member of staff allowing access to an unauthorised person, deliberately or inadvertently may be subject to disciplinary proceedings
- Staff may not connect any supplied equipment to any phone line, Internet connection or other computer, other than where they have been given authority and access to either the NHSnet or the Trust's network via a secure remote link. Any equipment supplied for remote access to the NHS network or the organisation must be stored securely when not in use
- Where a system requires a PIN number and a 'security token' or Smartcard these must be stored separately
- Staff should ensure that if they are using Trust equipment at home that their personal insurance covers them for the loss of any equipment provided by the Trust
- Storing person identifiable data files on portable devices is discouraged. Any identifiable or sensitive data stored on portable devices should have additional protection against unauthorised access and should be removed as soon as possible. If equipment has been used on a temporary basis then all data should be removed before return
- IT equipment must be transported in a secure, clean environment
- Provided all policy statements above are adhered to, staff may use any supplied equipment for any type of work which would normally be done on a Trust desktop PC, including the use of confidential information, provided there is compliance with general regulations on handling and storing confidential data and Trust policies

Homeworkers

- Only authorised members of staff are permitted to access NHS information in any form, on any media. Use of any information at home must be related to work purposes only. Staff must ensure the security of information within their home. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). Any person identifiable or Trust confidential information that has to be taken home must be within folders marked 'Private and Confidential' and kept secure when not in use
- Any staff who need to work from person identifiable or Trust sensitive data at home must receive formal authorisation from their senior manager. This

applies whether the data is to be removed in paper or electronic form

10.4 Malicious Software and Security Patches

Malicious software (Malware) may be defined as any unauthorised software introduced onto an IT system that is intended to cause harm to that system, or the data stored on that system. Malware is commonly but not exclusively referred to as computer viruses.

They can be introduced from the internet, on email attachments or on infected removable media. In addition to Malware, the network receives a threat from junk email, also known as spam. Whilst most spam is harmless, it can contain malware that is triggered when the message or attachment is opened.

SSHIS are responsible for updating and deploying anti-malware software and security patching. This includes issuing process documents for this activity. Removal of such software is not permitted.

10.5 Data Backup and Recovery

Periodically, information stored on our computers may become unavailable for a variety of reasons, e.g. the accidental deletion of a file by a member of staff, the technical failure of a hard drive or other storage media, or infection by malware. To minimize, the risk of this loss, SSHIS will perform backups on key data.

When a member of staff needs to recover any data, they should contact the SSHIS using the SMT portal and provide as much information about the file as possible. Staff should be aware that the recovery of information cannot be guaranteed, and any email or version of an email, that has been received, created or amended, and then subsequently deleted on the same day, i.e. between backups, may not be able to be recovered. Additionally, any information that is only stored on local drives or removable media cannot be recovered.

10.6 Penetration Testing and Vulnerability Scanning

A penetration test is an authorised simulated attack on a computer system, performed to evaluate the security of the system. The test is performed to identify weaknesses (vulnerabilities), including the potential for unauthorised parties to gain access to the system's features and data, as well as strengths and enabling a full risk assessment to be completed. The Trust has at least one authorised penetration test annually; it may also include a penetration test conducted under contract of NHS Digital.

The Security Operation Centre (SOC) will run periodic internal vulnerability scans using the NESSUS tool monthly. Results of these scans will be addressed in accordance with the risk posed to the Trust. The SOC will use the Common Vulnerability Scoring System (CVSS) and Vulnerability Priority Rating (VPR) to aid in setting patching guidelines.

10.7 Cryptography Controls

The following cryptographic controls that must be applied to Trust information:

General Principles

Extreme care must be taken to protect our information systems and assets to prevent unauthorised access by applying where applicable, a level of encryption to sensitive or

critical information which is proportionate to the Trust's risks.

All Confidential Information transferred outside of the Trust must be encrypted prior to transfer.

All removable media, including memory sticks, must be encrypted. Pre-encrypted memory sticks are approved for use on the network.

Mobile devices (laptops, tablets, digital cameras, mobile phones, CD/DVD writers, micro SD cards, scanners – this list is not exhaustive) must be protected by encryption and accessed via password and/or PIN numbers. New mobile computing devices received by SSHIS will be encrypted during the build process and before delivery to staff.

Personal unencrypted devices will be prompted to encrypt and the process cannot be reversed. NHS devices that are not encrypted will be prompted on connection to the network – failure to follow the on-screen instructions will render the device unusable on the network.

Encryption of Data in Transit

Confidential information in transit either physically or electronically must always be encrypted. Data which is already in the public domain (or would be of no adverse significance if it were to be so) may be sent unencrypted.

Encryption of Data transferred outside of the UK

Regulatory controls for any country to which data is exported outside of the UK should be checked to ensure that cryptographic legislation is not contravened, e.g. the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Where this is proposed IG staff should be consulted for approval before the transfer or travel.

11. Storing Information

As members of staff create documents, they will have a requirement to save them. However, it is important that documents are saved in a way where they can be backed up and recovered if the original document is accidently deleted, corrupted or otherwise lost.

The most common options for storing documents are detailed below:

Location	Benefits	Risks and Restrictions
Desktops	Convenient file access. Documents are available when the computer is not connected to the network.	Documents may not be recoverable if the hard drive fails as they are not backed up. Documents are normally only available on the computer where the document is stored. Documents subject to version control may lose that control if only stored on this manner. Local hard drives must not be used to store business critical documentation that is required by multiple members of staff.
Shared network folders (X drive)	Convenient file access. Access is controlled by security policy Documents available from any computer. All documents are backed up Familiar to Staff and requires no training.	Access to the document may not be possible during network disruption.
Home (or personal) network folders (U drive) Like shared network folders but the default security permissions limit access to the account holder only. These folders are limited in size. They are to be used to store personal work-related information that other members of staff will not need to access.	Convenient file access. Access is controlled by security policy Documents available from any computer. All documents are backed up Familiar to Staff and requires no training	Access to the document may not be possible during network disruption. Owing to the security permissions, only that named member of staff can access the information in it.

Location	Benefits	Risks and Restrictions
Removable Media	Convenient file access. Documents available on any computer. Any user of the media may access the document.	Does not provide users with any security controls as any user of the media may access the document. Documents are not backed up and may not be recoverable if the media fails or is lost. Documents subject to version control may lose that control if only stored on this manner. Must not be used to store business critical documentation that is required by multiple members of staff, unless all those staff have the necessary access.
Microsoft Office365	Convenient file access Documents available on any computer which has an Internet link It is designed for collaboration and sharing documents and data in many forms. E.g. One Drive, Teams Access is controlled by security permissions Access to documents from mobile devices	Vulnerable when the network or Internet is disrupted, as access to the documents may not be possible. There are still concerns in relation to user support; training and pilot sites are on a self-support basis.

11.1 Explicit Restrictions on Storage

The following locations must not be used to store Trust data:

- Any privately-owned device (including smartphones or removable media
- Any privately controlled cloud storage or email account

12. Removable Media

This paragraph introduces a series of restrictions when using removable media, where it is appropriate they must be adhered to.

Removable media is a means to transfer data, it is not intended to be a long-term storage medium, nor is it an adequate back up device. Removable Media should only be used to transport information when other more secure means are not available.

12.1 Restrictions for Storing Confidential Information on Removable Media

In order to prevent compromise or loss of Trust information, the following mandatory restrictions will apply to the storage of confidential information on removable media:

- When information is stored on removable media it is at its highest risk of compromise. Therefore, before storing any confidential information on removable media, members of staff are to exercise their professional judgement to determine whether or not the storage is appropriate and it is the only effective means available to transfer the information. *If other more secure means exist, they must be used.*
- Confidential information must only be stored on *approved secure* removable media, or by using approved encryption software that has been provided
- Confidential information is to be *copied* onto removable media. The original version is to be stored elsewhere on an appropriate network storage folder.
- Passwords must not be written down anywhere or disclosed to members of staff who do not have a need to know the material stored thereon.
- Removable media must not be used for the bulk transfer of data off site without the permission of the Trust's DPO.

12.2 Additional Restrictions for all items of Removable Media

In order to prevent compromise or loss of Trust information, the following mandatory restrictions will apply to all items of removable media:

- When information stored on an item of removable media is no longer required, it is to be deleted from the removable media
- When removable media is taken from Trust premises and is in transit, it is to be secured on the person of the individual removing it
- When removable media is taken from Trust premises and is being held on private premises, it is to be secured under "lock and key" when not in use
- All removal media is to be afforded the same level of physical protection as the most sensitive information saved thereon

- If any item of removable media is no longer required by the Trust, it must be destroyed by approved secure means
- Any loss or theft of any item of removable media must be reported immediately to SSHIS so that the level of compromise can be assessed, and necessary efforts can be made for recovery

12.3 Connecting Removable Media

This paragraph introduces guidance for connecting removable media to our network and to computers owned by other organisations and companies.

Using our Removable Media on non-Trust Computers

Removable media owned by the Trust may be connected non-Trust owned computers where a legitimate professional reason exists *and* the permission of the host has been given before doing so. If a legitimate professional relationship does not exist, the removable media is not to be connected.

Connecting Third Party Removable Media to our Computers

Removable media owned by other companies or individuals may be connected to Trust- owned computers but only where a legitimate professional reason exists. If a legitimate professional relationship does not exist, the removable media is not to be connected.

All files are swept for viruses when they are accessed but if a third party's removable media is used on our computer and a virus alert is generated, the member of staff is to stop using the device and inform SSHIS Immediately.

Examples of Legitimate Professional Reasons

Whilst in all cases, the member of staff concerned will have to make the decision as to whether or not a legitimate professional reason exists; it may be defined by using the following examples:

Example A
A clinician is giving a lecture to medical students at a local university and uses a PowerPoint presentation to aid this lecture.

The clinician may connect their removable media to the university computer provided that their permission is given.

Example B
A manager is meeting with representatives from partner organisations at their premises and they need to work together on a confidential business document as part of an on-going project.

The manager may connect their removable media to the host's computer as long as the partner has a legitimate reason to see the document and their permission is given. In this example, approved secure media must be used.

Example C
A company sales representative visits Trust premises to give a presentation to several members of staff and they have a demonstration version of their product on a USB

memory stick.

The representative may connect their removable media to our computer to demonstrate their product. This is a legitimate professional reason.

Example D
During a visit by colleagues from another Trust, they say that they have an electronic version of a recent research document on a memory stick. The member of our staff does not have a copy of this document that would be useful for their work.

As the document is for professional use, the memory stick may be connected to our computers in order to copy the document.

Example E
A member of staff has saved a private letter to a privately-owned memory stick and they bring it to work to print it.

As no legitimate professional reason exists, the memory stick is not to be connected to our computers.

12.4 The Procurement and Availability of Removable Media

The procurement of removable media is only to be carried out by SSHIS and, where possible, only approved secure removable media as defined by the Chief Information Officer/Deputy Chief Information Officer are to be procured.

Only secure USB memory sticks provided by SSHIS are approved for use to hold confidential information.

13. Access Controls

13.1 Computer System Access Control

Line managers must ensure that only authorised staff i.e. appropriate to their role, have access to information, hardware and software. Access authorisation should be regularly reviewed, particularly when staff roles and responsibilities change.

Controls are in place to ensure that only personal with the proper authorisation and a need to know are granted access to systems and resources. These controls authenticate the identity of users and validate each user's authorisation before allowing users to access information or services on the system. Information used for authentication is protected from unauthorised access.

Portable computing equipment will only be issued to staff where there is a demonstrable need for them to capture or process information away from a fixed base. Service managers must identify and justify the use of portable computing equipment when defining and appointing to posts and must notify this requirement to SSHIS as part of new starter arrangements. Service managers must also notify the SSHIS when a subsequent role change affects the need to use portable equipment.

Regardless of a laptop's ownership, the use of any equipment outside an NHS organisation's business premises for the processing of NHS information must be authorised by the relevant Director or Head of Department.

Where the processing of NHS patient information is proposed on laptop devices additional authorisation must be obtained from the organisation's Caldicott Guardian. In exceptional situations a Senior Manager can give explicit documented approval for the use of personal identifiable or sensitive data away from the normal workplace. In this eventuality the Senior Manager is responsible for ensuring the security of such information.

Any data security incident where Trust policy and procedure has been violated by staff may be subject to formal disciplinary action under the Trust's Human Resource policy framework and, if considered sufficiently serious, may constitute grounds for dismissal.

13.2 Prevention of Misuse

Any use of Trust computer facilities for non-business or unauthorised uses without management approval will be regarded as inappropriate usage.

The Computer Misuse Act 1990 introduced three criminal offences. Staff must remember that the following offences can be enforced in a court of law:

- Unauthorised access
- Unauthorised access with intent to commit further serious offence
- Unauthorised modification of computer material

13.3 Obtaining a Network Account

It is NHS policy that all staff should have access to Electronic Mail. To use email you require a network account. You also require an account to access applications such as Lorenzo, ESR etc.

A potential new user and their line manager should complete an ***Application for Network Account Form***, available on the Intranet.

13.4 Closing a Network Account

Managers should notify SSHIS of all leavers so that their network account can be disabled. Emails are retained on a leavers Outlook account for 12 months and then permanently deleted.

13.5 Training

It is the responsibility of line managers to ensure that all staff receives appropriate training in the use of the IT systems for which they have been given access.

13.6 Remote Access Service

Remote access will be controlled through identification and two factor authentication mechanisms. No confidential information may be copied from Trust network drives to non-Trust equipment (e.g. home computers) for processing.

This service is dependent upon:

- A Trust device with membership of the appropriate security group
- A pre-installed and configured digital certificate
- A broadband connection (NHS, public or private)

The following restrictions may apply to this service:

- When at home, the provision of this service is limited by the availability of a

suitable broadband service. As the availability, speed and reliability of these services are beyond the control of the Trust, the availability of the Service cannot be guaranteed

- You may connect to publicly available internet connections, even though they are not shown as secure, without permission. The service creates its own encrypted connections
- The permission of any NHS third party host, e.g. a GP surgery, must be sought before attempting to connect using their network infrastructure
- SSHIS are not responsible for resolving faults affecting third party broadband services, e.g. at a GP surgery, WIFI Hotspot or at home.
- SSHIS will not make visits to non-Trust premises, e.g. a member of staff's home.
- Out of normal business hours, faults should continue to be reported but will only be addressed if the fault is affecting the service as a whole, not just an individual member of staff
- When working in public places or domestic environments, members of staff are to ensure that unauthorised persons cannot oversee any information that is displayed on their screen

13.7 Third Party Access

Third parties will not be given access to systems or networks unless the Trust/persons in question have formal authorisation to do so. All non-NHS companies will be required to sign security and confidentiality agreements with the Trust – these must be signed before access is assigned.

When permitting access to our network the following principles will apply:

- Access will only be granted after a valid request has been evaluated by a DPIA
- When permission is granted, access rights will be assigned using the principle of 'least privilege', i.e. only granting the lowest level of access necessary for the third party to effectively do their job
- When there is any doubt over the level of access rights, the Chief Information Officer/Deputy Chief Information Officer will have the final decision as to the appropriate level
- Access rights will only be granted for the duration of the contract or period of support and will be withdrawn when they are no longer required
- All solutions must include the ability for SSHIS to end the connection without any requirement for the third party to take any given action, i.e. a unilateral kill switch

Third parties found accessing elements of the system that they are not authorised to, will be deemed a security breach and will be denied access immediately. An investigation will take place to decide the outcome.

14. Use of Email

Email is provided to staff as a business tool, but because of its potential for misuse and abuse it is necessary to have in place a range of rules / guidelines to promote acceptable use for the protection of both the user and the Trust. These rules and guidelines are based on current legislation and common-sense principles. Their purpose is:

- To ensure that email is used effectively, an understanding of how it works and of good practice and etiquette that applies to its use
- To protect the users and the Trust from the risk of legal liability as a result of email abuse
- To protect and maintain the quality of Trust information against threats via external intrusion

14.1 Long-Term Absence

If a staff member is on long-term absence (more than four weeks), their line manager should with the help of SSHIS, redirect the account to someone else within the department who has authority to manage that account. The justification of redirecting the messages should be clearly established prior to redirection. The duty of confidentiality should be impressed upon the member of staff who receives the redirected mail.

14.2 General Rules

Properly used, email can be an immense benefit to the NHS and its staff. The following rules apply to anyone using the Trust's IT systems to send and receive email and the posting of information on the Trust's Web Pages:-

- Confidential person-identifiable information should not be distributed by email unless there is a specific requirement for it. Casual disclosure of personal details of patient, employee, volunteer or contractor without just cause may be considered a breach of personal privacy as defined under the Data Protection Act
- Patient identifiable data must not be sent to a personal (non-NHS) email address without additional security such as 'encryption'. Commercial internet email services are not secure and should not be used to send person-identifiable (patient and staff), confidential material or governance classified information
- Staff must not automatically forward emails from their work email address account to a commercial email address for access at home
- If however you need to send such information see the **'Secure Email Guidance'** document on the Trust intranet for clear direction on what secure method to use
- Log in at least twice daily, if not all day, and respond to requests within a reasonable time
- Advise people when you are not available. Use the tools within your system (i.e. Out Of Office Assistant) to notify others of your inability to read your email
- Set up a Signature with your name, organisation, telephone number, other useful contact information and a legal disclaimer
- As people may receive many email messages it is important that a subject is added to the email in order that the recipient can clearly see what the email is about. It will also assist the recipient in prioritising opening of emails
- Ensure that you are sending the email to the correct person. If in doubt, confirm their email address with them
- Use the spell checker before you send out an email
- Emails should be treated like any other correspondence and should be replied to within an acceptable time limit
- Only send emails if the content would be suitable for display on a public notice board or the Trust's publication scheme. If they cannot be displayed publicly in their current state, consider rephrasing the email or using other means of communication

- Use distribution lists with care – is it important that all addressees receive the email? Only use organisation-wide distribution lists to communicate important business information that has genuine site-wide value
- Update your email groups at regular intervals. Check for leavers or members who have moved on into another role – it may not be appropriate for them to continue to receive emails from the group and may lead to a breach of the DPA
- Type your message in lower case. Using capital letters is considered aggressive

14.3 Do's and Don'ts of Email

- Staff must not send any message which is abusive, offensive, obscene or potentially defamatory or which consists of gossip. Comments of this nature can be construed as harassment. Ensure that all statements and comments you make about people or organisations are true (*Computer Misuse Act 1990*)
- Remember that the email system is for business use. You may, however, make sensible use of it for non-business purposes. Use your common sense if you send personal messages to other members of staff via this system. Bear in mind that you should not be spending more than a minimal amount of time on matters unrelated to your work. Be aware that unauthorised and excessive use of any means of electronic communications by staff at the Trust is a disciplinary offence
- Take extreme caution when disclosing your Trust Internet email addresses to outside organisations. The addresses may be misused or sold on and as a result cause an influx of junk mail
- Do not circulate jokes; computer programmes (executable files) documents such as chain letters, celebratory greetings messages (e.g. animated Christmas cards), music, video and photographs. Circulating such material can pose serious business and operational risks by using up excessive storage space and may infect PCs or servers with viruses
- Anonymous messages are not permitted. Do not attempt to send messages purporting to come from another individual or email account without written consent
- If you send personal messages you must take care that they cannot be confused with Trust business communications
- Do not present views on behalf of the Trust, unless you are authorised to do so
- Be mindful when deleting emails permanently, as under the Freedom of Information Act, you may need to refer back to such communications or provide as evidence in responding to Freedom of Information requests
- Do not send large attachments by email. Place large attachments in a shared location (where possible) and then send just the file path via an email. If you believe that most recipients will print the document, try to use another method of sending the hard copy
- Do not attach files to emails from unknown sources (may contain viruses). Do not open file attachments with possible virus warnings. If you suspect you received a virus by email, telephone SSHIS immediately. Do not attempt to remove the virus yourself. SSHIS will need to know what virus it is
- Keep the Inbox to a minimum and adhere to good housekeeping practices. Create a personal folder structure under different headings. Transfer email from the Inbox to the appropriate folder on regular basis
- Review saved emails every month and delete any that are no longer required. If there is an email that may be required in the future, it should be archived

14.4 IT Access to Email Messages

SSHIS do not routinely monitor individual email accounts or email messages. However,

in order to maintain the availability of the email system, there may be occasions when SSHIS have to access a mailbox for maintenance and housekeeping purposes e.g. if a mailbox has reached its maximum size, staff changes etc. Such access will not be used to review the content of individual email messages.

14.5 Individuals' Rights to Access Email Messages

The Data Protection Act gives individuals the right to access any information held on them, including email messages. (*Access to Health & Employee Records Policy 7.02*). In addition, the Courts and Employment Tribunals have the power to order disclosure of emails that may be relevant to a case. This emphasises the point that emails are more than just an electronic conversation. Messages should be taken seriously and the content should be in accordance with the principles of the Data Protection Act, GDPR and the Caldicott recommendations.

14.6 Malicious Communications

The Malicious Communications Act 1988 makes it illegal in England and Wales to "send or deliver letters or other articles for the purpose of causing distress or anxiety".

a) a letter, electronic communication or article of any description which conveys—

   i. a message which is indecent or grossly offensive; a threat; or

   ii. information which is false and known or believed to be false by the sender; or

b) any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature

Is guilty of an offence if his purpose or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

14.7 Copyright

Email messages may contain or attach copyright work owned by a third party. If you make an electronic copy of such work you may be infringing copyright (Copyright, Patents & Designs Act 1988). It is an offence to copy any item of software without the owner's prior permission. The use of illegal or unauthorised software on a Trust computer is a breach of this policy.

15. Internet Access

All sections of this policy apply to all Internet access using any NHS resources. Violation of this section will be grounds for having access to the Internet restricted or revoked.

It is clear that Internet access can be a valuable tool to staff throughout the Trust, both within their normal work activity and as an aid to learning. Furthermore, the Internet is also a route by which to deliver information and guidance to patients and to the public.

Potential Problems

There are a vast number of sites that the Trust would not wish employees to access. We must equip ourselves with a set of security measures which will minimise the risks to our resources from external intruders and which will both deter and detect employees who access 'inappropriate' Web sites. The definition of 'inappropriate' is anything that may cause offence to other individuals. **The Trust has the ability to**

monitor Web sites that user's access and does so on a regular basis. It is the responsibility of a user's line manager to give the user Internet access rights or to take those rights away.

Breaches of this policy will be brought to the attention of a user's line manager and to the appropriate senior manager.

Responsibilities of the User

It is the responsibility of all staff within the Trust to ensure that the computer systems and the data that is accessed through them are safe and secure. Staff that uses the Internet have additional responsibilities relating to security, confidentiality and inappropriate use.

Permissible Access

Access to the Internet is primarily for healthcare related purposes. That is for Trust work or for professional development and training. Reasonable personal use is permitted provided that this does not interfere with the performance of your duties and is carried out during official work breaks e.g. lunchtime or outside of core working hours. The Trust has the final decision on deciding what constitutes excessive use.

Non-Permissible Access

No member of staff is permitted to use Trust provided internet connections for any of the following:

- Using another person's account or identity to access the Internet, either with or without their permission
- Attempting to download any unauthorised software, programmes or executable files
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- Audio and/or video streaming for non-work purposes, e.g. listening to the radio via the Internet
- Disclosing any patient identifiable information, business information or other confidential information on any unauthorised web site, forum or similar site
- Placing libellous, defamatory or otherwise derogatory comments on authorised Trust or any other web forum, social network or similar sites
- Harassing or bullying other members of staff as defined by Trust policy
- Operating or managing any business other than that of the Trust, except where contractually agreed with partner organisations
- Additionally, you must not intentionally access, download, store, process, display, distribute or send material, images or pseudo-images relating to the following:

    - Fraud, illegal activities, malicious activities (including computer hacking and/or software, film or music piracy)
    - Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no authorised connection with the Trust.
    - *Note: The use of Trust Internet facilities by Trade Unions or other recognised professional bodies or organisations is permitted*

- Offensive, obscene or derogatory material that is pornographic, sexist, racist or otherwise inappropriate in nature
- Dating, escort, gambling or similar industries
- Sites promoting the inappropriate use of illicit drugs (except where this is specifically related to the execution of your duties)
- Audio and/or video download or retail sites (irrespective of whether or not a fee is charged)

Unintentional Breaches of Security

If you unintentionally find yourself connected to a site that contains sexually explicit or otherwise offensive material, you must disconnect from the site immediately and inform your line manager and SSHIS.

Personal Details

It is recommended that members of staff do not disclose any of their personal details over the Internet whilst using Trust facilities. These details may include:

- Demographic information
- Banking or other financial details
- Account and associated passwords

The Trust cannot be held liable for any loss related to the disclosure of any personal details that have been wilfully compromised in such a manner.

Accessing the Internet via Mobile Devices

When staff access the Internet or World Wide Web using mobile computing devices such as SmartPhones or Tablet PCs and that access is gained using a Trust network (including wireless), an audit trail of sites visited is maintained centrally by the IT Service. When access is gained through a home broadband connection, an audit trail may remain on the device.

16. Bring Your Own Device (Non-Clinical Only)

Bring your own device (BYOD) is now available for **corporate staff that do not work with clinical data.** To improve security and to ensure that Trust information is not stored inappropriately, personal devices must be enrolled. This allows us to mandate certain security features such as ensuring a pin set on the device and that encryption is enabled. This also allows us to remove Trust data from a personal device when staff no longer work for us.

Enrolling your device will allow you to use Apps to access your work email, OneDrive, Teams etc on your personal device. If you do not wish to enrol your device, you must use your work device to access Trust information.

Your personal device must be capable of receiving the latest OS/security updates (and you should have applied them), to be accepted for enrolment.

We reserve the right to deny access to work O365 systems if your personal device is running versions of software and operating systems that are not secure – this includes devices declared obsolete by the manufacturer/OS provider and therefore not receiving security updates.

We have the right to remotely wipe Trust information from your personal device if it poses a risk to the organisation or its data.

The Trust and S&SHIS cannot see your personal information when you enrol your device.

We only have the ability to manage the applications and accounts that are installed for the Trust – we will not be monitoring your activity.

What we can see	What we can't see
Device Owner & Device Name	Calling and web browsing history
Device Serial Number	Email and text messages
Device Model	Contacts
Device Manufacturer	Calendar
Operating system and version	Passwords
Device IMEI	Pictures, including what's in the photo app or camera roll
App inventory and app names for managed work apps	Files

The Trust remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing.

BYOD User Responsibilities

- Familiarise yourself of your device and its security features so you can ensure the safety of Trust information
- Invoke relevant security features
- Ensure that your personal device is not used for any purpose that would be at odds with our IT and data protection policies
- Ensure that the device is not used for illegal activities
- Ensure that accounts are logged out of when not in use
- Ensure that no other person accesses Trust information
- Prevent theft and loss of data and report any loss to S&SHIS as soon as you become aware so that the device can be wiped of Trust information
- Keep Trust information confidential where appropriate
- Take responsibly for any software you download onto your device
- Ensure that personal devices do not hold any data that is sensitive, personal, confidential or of commercial value
- Not use any device that has had its terms of service broken, such as a 'jailbroken' device

17. Roles and Responsibilities

Chief Executive

The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for information security in the Trust and is required to provide assurance through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated. Details of Serious Untoward Incidents involving data loss or confidentiality breach must also be reported in the annual report.

Senior Information Risk Owner (SIRO)

The Director of Finance is responsible to the Chief Executive for information security and is the designated Senior Information Risk Owner (SIRO), who takes ownership of the Trust's Information Risk Policy, acts as advocate for information risk on the Board and provides written advice to the Accountable Officer on the content of the Statement of Internal Control in regard to information risk.

The SIRO is also required to undertaken additional information security training relevant to their responsibilities.

Caldicott Guardian

The Caldicott Guardian is the “conscience” of the organisation, providing a focal point for patient confidentiality and information sharing issues, and advising on the options for lawful and ethical processing of information as required. The Caldicott Guardian and SIRO are both concerned with ensuring NHS data is protected and is not stored, accessed or used inappropriately. The SIRO and any organisational IAOs work closely with the Caldicott Guardian and consult him/her where appropriate when conducting information risk reviews for assets which comprise or contain patient information. In most NHS Trusts the Caldicott Guardian is the Medical Director.

The Caldicott Guardian will authorise access on key issues such as sharing information and the protection and use of patient-identifiable information. The Caldicott Guardian will also advise the Trust Board on progress and issues as they arise.

The Caldicott Guardian is also required to undertaken additional information security training relevant to their responsibilities.

Chief Information Officer/Deputy Chief Information Officer

The CIO and DCIO are responsible to the SIRO and IAOs for the identification, delivery and management of an information risk management programme to address and manage risk to the Trust’s assets.

They provide assistance on implanting controls for staff members that do not work in the usual Trust workplace.

Data Protection Officer (DPO)

The Data Protection Officer interprets national guidance and legislation to develop policy, strategy and systems to ensure compliance with Information Governance Data Protection requirements and the achievement of data quality standards in line with the GDPR, providing leadership, challenge and support to achieve organisational compliance.

Information Asset Owners (IAOs)

Appropriate staff will be designated Information Asset Owners (IAOs) with responsibility for the completion and maintenance of the Trust’s Information Asset Register; for completing audits of their assigned assets on an annual basis as evidence for the Data Security Protection Toolkit; for providing assurance to the SIRO that information risks within their respective directorate have been identified and recorded and that controls are in place to mitigate those risks.

The IAOs are also required to undertaken additional information security training relevant to their responsibilities.

Information Asset Administrators (IAAs)

IAOs can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities for the Directorate. IAAs ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

The IAAs are also required to undertaken additional information security training relevant to their responsibilities.

Managers

Managers are responsible for ensuring that:

- Information security breaches are reported through the Trust incident reporting system (Safeguard), investigated and, where appropriate, disciplinary action taken
- Information Security breach reports are provided to the relevant committees as detailed in the Trust's risk management policy (4.18).
- All the requirements of this policy are implemented, managed and maintained in their business area
- Their staff are aware of their responsibilities and accountability for information security including the potential disciplinary actions for non-compliance and that they comply with controls that are in place
- Their staff complete information security training on an annual basis as part of their mandatory training suite
- New staff complete their Trust induction which includes an overview of information security responsibilities and controls
- Local detailed processes are developed and implemented to maintain information security
- Only approved software is used on equipment that processes information. New software, which has not been properly developed and/or properly tested, is a threat to the security of existing data. All software and hardware procurements shall take account of the Trusts security requirements. This shall specifically include the procedures and actions for handing over and testing new software. Contravention of the recommendations may be considered a disciplinary offence
- Retention periods for documents relevant to each Department/Directorate via the Trust's Records Management Policy 7.07, which includes reference to the safe destruction of documents are maintained
- System training is provided prior to users operating any clinical system, according to the access level required
- All redundant and unwanted IT hardware and related media is returned to SSHIS for safe disposal
- Staff who remove information in any form or use information in any form away from the usual Trust workplace are aware and comply with this policy
- Service Managers and internal auditors are responsible for assessing risks and ensuring that controls are being applied effectively
- SSHIS are informed if:
    - IT equipment is transferred to another area
    - Staff circumstances change as it may affect access to systems
    - New software and hardware are required
    - Prior to operating any clinical systems all potential users, including temporary/agency staff, must receive system training according to the access level required

Data Protection Steering Group

Overall responsibility for confirming whether remote access to business applications and systems is permitted away from the usual Trust workplace

Staffordshire & Shropshire Health Informatics Service (SSHIS)

The Staffordshire & Shropshire Health Informatics Service (SSHIS) will provide appropriate management information in relation to IT and IT related equipment and software.

Staff

Information security and the appropriate protection of information assets, which includes information in emails and the email system, is everyone's responsibility.

All staff are obliged to:

- Comply with this policy and support its objectives
- Complete their annual information security awareness training
- Ensure that they understand their responsibilities around information security and comply with the law
- Report information security incidents via the Trust's incident reporting system (Safeguard)
- Ensure that they do not save files that contain offensive material. To do so may constitute a serious breach of Trust security and could result in dismissal and/or criminal prosecution. The Trust is the final arbiter on what is or is not offensive material
- Ensure that data quality is maintained
- Failure to comply with this policy is a disciplinary offence
- Ensure that they do not install software onto a Trust owned device. SSHIS conduct audits of all software and if unauthorised/and or unlicensed software has been purchased, they are authorised to remove it
- Advise SSHIS if there is a suspicion that unauthorised software is present on your asset
- Ensure that anti-virus software is installed and active – contact SSHIS for advice
- Lock your computer when leaving it unattended

Staff that work away from the usual Trust workplace

In addition to the responsibilities above:

- Keep usage to a minimum in public areas
- Only access information off-site/at home for work-related purposes
- Ensure security of information within the home or off-site
- Not connect any Trust supplied equipment to any computer network other than the NHS network or the Trust's network other than by using the secure access procedure. This includes the use of Wireless Access Points often found in public buildings
- Not use patient identifiable or staff identifiable data on any equipment not provided by the Trust
- Not send patient or staff identifiable data to home (Internet) email addresses. • Keep equipment, media and files including paper locked out of sight during transit
- Ensure equipment and files are adequately packaged in transit to prevent damage or tampering
- Not dispose of any media containing sensitive/confidential information (including paper) off-site. All such information must be returned to a Trust-owned location

for safe disposal

18. Monitoring and compliance

The Trust reserves the right to monitor work processes to ensure the effectiveness of the services provided. This will mean that any personal activities that any employee engages in during work time may come under scrutiny. It will respect the privacy of its employees and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

Managers are expected to speak to staff of their concerns should any minor issues arise. If serious breaches are detected an investigation must take place. Where this or another policy is found to have been breached the relevant Trust procedures will be followed.

Concerns about possible fraud and or corruption should be reported to the Counter Fraud Department.

In order for the Trust to achieve good information governance practices, staff must be encouraged to recognise the importance of good governance and report any breaches or incidents to enable lessons to be learned. Staff must be provided with the necessary tools, support, knowledge and training to help them deliver their services in compliance with legislation. Ultimately a skilled workforce will have the confidence to challenge bad information governance practices and understand how to use information legally in the right place and at the right time. This should minimise the risk of incidents occurring or recurring.

19. Review

This policy will be reviewed every two years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Changes in systems/technology; or
- Changing methodology.

Any updates and amendments to this Policy will be recorded in the document control section in Appendix B.

Appendix A: Definitions

Term	Description
Asset Register	Essentially a list of an organisation's assets and their condition and helps an organisation to ascertain what it owns or leases and the stock of that item.
Business Continuity	The ability of an organization to maintain essential functions during, as well as after, a disaster has occurred.
Common Law Principle of Confidentiality	Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges and is also referred to as 'judge-made' or case law. The law is applied by reference to previous cases and is said to be 'based on precedent'.
Consequence	The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.
Data Protection Impact Assessment	A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
Data Protection Officer	Legally accountable to the Information Commissioner's Office and responsible to the SIRO to ensure that the Trust processes its personal and special category data lawfully and its information risks are correctly managed.
Data Security and Protection Toolkit	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian`s 10 data security standards.
Digital Certificate	Used to encrypt online data/information communications between an end-users browser and a website.
Disaster Recovery	Involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
Freedom of Information Act	An Act of Parliament of the Parliament of the United Kingdom that creates a public "right of access" to information held by public authorities.
General Data Protection Regulation	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.
Hardware	Describes the physical aspects of a computer/device.
Information Asset Administrator	A term given to staff, typically within ICT, who actively support the maintenance and operation of a given information asset.
Information Asset Owner	A senior member of staff with responsibility for the management of a given information asset within their area of responsibility.
Least Privilege	Only granting the lowest level of access necessary for the third party to effectively do their job.

Term	Description
Likelihood	A qualitative description or synonym for probability or frequency.
Malicious Software	Also known as malware, is any software that does harm to the system, such as a virus or spyware.
Malicious software attacks	Also known as malware, is any software that does harm to the system, such as a virus or spyware.
National Data Guardian for Health and Care	An independent, non-regulatory, advice giving body in England sponsored by the Department of Health and Social Care.
Recovery Point Objective (RPO)	The agreed point in time before the disruption to which information should be recovered to within the RTO.
Recovery Time Objective (RTO)	Target time for services to be restored to an agreed state following disruption.
Remote Access Service	Any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
Risk	The chance of something happening which will have an impact upon objectives. It is measured in terms of consequence and likelihood.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Risk Management Process	The systematic application of management policies, procedures and practices to the task of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.
Security Patching or Patch	Set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs.
Serious Incident Requiring investigation	Incident where one or more patients, staff members, visitors or member of the public experience serious or permanent harm, alleged abuse or a service provision is threatened.
Software	A set of instructions, data or programs used to operate computers and execute specific tasks. Software is a generic term used to refer to applications, scripts and programs that run on a device
Software Update(s)	An update is new, improved, or fixed software, which replaces older versions of the same software
Spam	Refers to the use of electronic messaging systems to send out unrequested or unwanted messages in bulk.
Special Category Data	Personal data is any information that relates to an identified or identifiable living individual.
Viruses	Type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code

Appendix B: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
29/09/2022	1	Head of Information Governance	Full rewrite of Information Security Policy incorporating IT Assets, Information Risk and Mobile Information Handling to streamline and make more transparent and available for staff
25/10/2022	2	Head of Information Governance	Incorporating further information around BCP/DR and Social Engineering
27.03.2024	3	Head of Information Governance	Adding section about 'Bring Your Own Device' (BYOD)

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
14/10/2022	1		Deputy Chief Information Officer
14/10/2022	1		Chief Information Officer
25/10/2022	2		Deputy Chief Information Officer
11.03.2024	3		Deputy Chief Information Officer

Approvers

This document requires the following approvals:

Date	Version	Name	Status
31.10.2022	v2	Data Protection Steering Group	Approved
		Senior Leadership Team	
12.03.2024	v3	SIRO & Caldicott Guardian	Approved
	v3	Senior Leadership Team	

Keele UNIVERSITY TEACHING TRUST

NHS North Staffordshire Combined Healthcare NHS Trust

Doc level: Trustwide
Code ref: 7.24

National Data Opt-Out Policy

Lead executive	Director of Partnerships, Strategy and Digital
Authors details	Head of Information Governance

Type of document	Policy
Target audience	North Staffordshire Combined Healthcare NHS Trust workforce
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet

Approval meeting	Finance and Performance Trust Board	Meeting date	31 March 2022 14th April 2022
Implementation date	15th April 2022	Review date	30 April 2025

Trust documents to be read in conjunction with	
Document code	Document name
7.08	Information Governance Policy
5.01	Incident Reporting Policy and Procedure Document

Document change history		Version	Date
What is different?	New Policy developed to meet requirements of Data Security and Protection Toolkit	1.0	10/01/2022

Training requirements	Information governance staff who are involved in determining when the National Data Opt-Out applies when sharing personal information for any reason that falls outside of direct patient care. Need for staff to rely on support from IG Team.

Document consultation	
Directorates	
Corporate services	
External agencies	

Financial resource implications	No

External references
1. Data Protection Act 2018 2. UK General Data Protection Regulations (UK GDPR)

Monitoring compliance with the processes outlined within this document	

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favourably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
– **Religion and/or Belief** (includes those with religion and /or belief and those with none)		
– **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)	No	
If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.		
Not Applicable		
If you have identified potential negative impact: - Can this impact be avoided?		

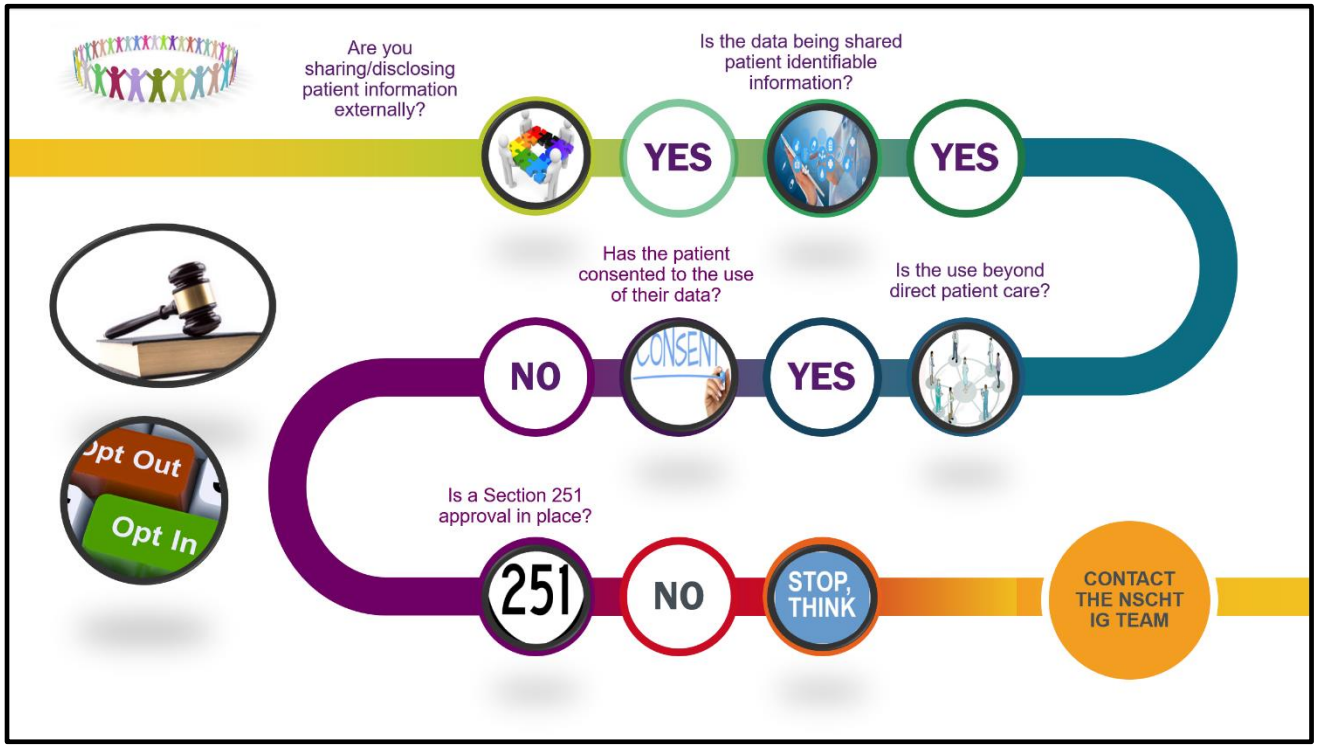
- What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?	
Not Applicable	
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A
Not Applicable	
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk	
Was a full impact assessment required?	No
What is the level of impact?	Low

Contents

National Data Opt-Out: A Quick Reference

Patients can opt out of their data being used for planning or research purposes under the National Data Opt-Out that was introduced on 25th May 2018. This is in line with the recommendations made by the National Data Guardian following a review of **Data Security, Consent and Opt-Outs**.

Staff sharing or disclosing confidential or sensitive patient information can use the below diagram or NHS Digital's guidance on When National Data Opt-Out Does Not Apply to identify whether national data opt-out applies or not. Where the national data opt-out applies, following the NHS Digital guidance When National Data Opt-Out Applies staff must contact the Information Governance Team who will provide the required support and guidance.



1.0 Introduction

In response to the National Data Guardian (NDG) review of data security and how health care organisations use and share data, the National Data Opt-Out (NDO) was developed. NDO will allow patients registered in England to control how their data is shared for secondary purposes outside of the initial purposes for which their information was collected.

North Staffordshire Combined Healthcare NHS Trust (NSCHT) has produced this National Data Opt-Out Policy to provide staff with the required information to assist in ensuring as a Trust we can demonstrate our compliance with this requirement as well as providing a robust framework to ensure a patient's opt-out choice is respected.

2.0 Scope

This policy applies to:

- Staff handling information at any NSCHT site including contract staff, bank workers, locums, students and volunteers.

- Technologies, hardware, software and peripheral equipment owned and provided by NSCHT.
- Information and data NSCHT holds in any format.
- New and developing technologies, which may not be explicitly referred to.

3.0 Definitions

Anonymised data: Data from which the patient cannot be identified by the recipient of the information.

Confidential or sensitive patient information: Information is when two types of patient information are joined together. The two types of information are a person's identity and information about his or her health care or treatment, for example, their name along with the treatment they received or their NHS number along with the medication given.

UK General Data Protection Regulation (UK GDPR): The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018. The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

Message Exchange for Social Care and Health (MESH): This tool is used to check patient opt-out choices against the national opt-out repository held on the NHS Spine. If opt-outs are found, the service will remove them and return a list of NHS numbers that you can use or disclose for the secondary purpose.

NHS Digital: Is the trading name of the Health and Social Care Information Centre, which is the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care in England, particularly those involved with the National Health Service of England. The organisation is an executive non-departmental public body of the Department of Health and Social Care.

Personal data: Shall mean any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Privacy and Data Protection Legislation: Shall mean all applicable laws and regulations relating to the processing of the personal data and privacy, including:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018
- The Human Rights Act 1998
- The Privacy and Electronic Communications Regulations 2003 (PECR)

Secondary purpose/secondary use: Any data use activities where the uses or purposes are other than direct or 'primary' clinical care for example healthcare planning, commissioning, clinical audit and governance, benchmarking, performance improvement, medical research and national policy development.

Section 251: The purpose of Section 251 is to enable the common law duty of confidentiality to be lifted, in order to allow disclosure of confidential information about patients for secondary purposes without the need to use anonymised data, and without the need to obtain consent.

Section 259: The purpose of Section 259 is to enable NHS Digital with statutory powers, to require data from organisations that provide health or adult social care in England.

Special Category Data: UK GDPR refers to sensitive personal data as "special categories of personal data" (defined in Article 9 UK GDPR). The special categories include but is not limited to health data, family, lifestyle and social circumstances, vulnerable individuals, education and training details, cultural identity including racial or ethnic origin, political opinions, religious or philosophical beliefs, location data, technology identifiers, sexual life, employment details, genetic data, and biometric data where processed to uniquely identify an individual.

4.0 Roles and Responsibilities

Accountable Officer: Overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

Senior Information Risk Owner: Ensure that all information risks are assessed and mitigated to an acceptable level. Provide the Accounting Officer with assurance that information risk is managed across the trust and by services contracted by NSCHT.

Caldicott Guardian: Ensure that procedures are in place to govern access to and the use of personal identifiable and confidential information. Provide leadership and informed guidance on complex matters involving confidentiality and information sharing. Oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies.

Executive Team: Supporting and adhering to this policy, ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Data Protection Steering Group: Ensure that this policy is implemented, monitored and reviewed by all members of this group to ensure data protection principles, especially around fairness and transparency, can be evidenced.

Data Protection Officer: Ensure that this policy is implemented, monitored and reviewed in line with legislative requirements and best practice.

All Managers: Ensure compliance with this policy and that the staff for whom they are responsible are aware of and adhere to this policy.

All Staff: Supporting and adhering to this policy, in particular:

- To seek advice from the Information Governance Team on whether the National Data Opt-Out applies to their data activities and how it can be implemented in their area.
- Every member of staff is responsible for taking precautions to ensure the security of information, both whilst it is in their possession and when it is being transferred from one person or organisation to another. If staff are unsure about sharing information, they should refer to the suite of Information Governance Policies or take advice from their line manager, the Information Governance Department or the Caldicott Guardian, as appropriate.
- Be aware of information risk management and understand the need for information risk to be a part of the trust culture.
- Are familiar with the data protection principles, Caldicott Guardian principles and documented procedures within this policy.
- Carry out day-to-day work in accordance with best practice confidentiality and data protection procedures and legislation.
- Keep up to date with best practice confidentiality and data protection procedures and legislation through undertaking annual Information Governance training.

- Understand and adhere to, the Privacy and Data Protection Legislation and other legal requirements including the Confidentiality NHS Code of Practice to support the Caldicott Guardian and safeguard against harm to individuals or the trust's reputation.

5.0 Process

NHS Digital have an example of the format of the data file that is required for processing through the Check for National Data Opt-outs Service, which can be accessed here:

https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out/check-for-national-data-opt-outs-service/format-of-nhs-number-data-file

5.1 Message Exchange for Social Care and Health (MESH)

NHS Digital has developed a technical service known as MESH, which enables any organisation registered for this service to check if patients have a national data opt-out applied.

The Trust/GP Practice can submit a list of NHS numbers that they need to disclose and the MESH service looks these up against the central repository of national data opt-outs. To support the data transfer via MESH, the dataset must contain NHS Numbers in a single column, separated by a carriage return.

The MESH service returns a "cleaned list" of those that do not have a national data opt-out i.e. it removes the NHS numbers for those with a national data opt-out.

5.2 For Patients

Patients can set or change their national data opt-out choice using an online or contact centre service. When a patient sets a national data opt-out it is in held in a repository on the NHS Spine against the patient's NHS number. National data opt-outs may take up to 21 days from being registered with NHS Digital to being fully applied to all disclosures of data.

Patients can view or change their national data opt-out choice at any time by using the online service at **www.nhs.uk/your-nhs-data-matters.**

Or by clicking on "Your Health" in the NHS App, and selecting "Choose if data from your health records is shared for research and planning".

5.3 Resources for patients

Staff can use the 'Your Data Matters to the NHS' resources at **https://digital.nhs.uk/services/national-data-opt-out/supporting-patients-information-and-resources** to help raise awareness.

5.4 For audit and research teams

Audit and research teams can direct staff who are sharing/disclosing confidential information to the diagram at the beginning of this policy or to the NHS Digital Guidance on National Data Opt-Outs. Where the national data opt-out applies, staff must contact the Information Governance team by e-mailing **NSCHT.InformationGovernance@combined.nhs.uk**

Depending of the nature of the request the Information Governance Team may request that a Data Protection Impact Assessment (DPIA) be completed.

6.0 Data Protection Impact Assessments (DPIA)

Risks to personal, confidential or sensitive information that arise as a result of must be further assessed and documented through the completion of Data Protection Impact Assessment (DPIA). The DPIA should be completed by a nominated Project Lead or suitable individual who is responsible for achieving the project objectives and outcomes.

The DPIA Briefing Note and Guidance produce to support staff in their undertakings sets out the basic steps which all staff should understand and must follow during the initiation phase or early assessment for the development, implementation of projects at NSCHT.

The DPIA process and briefing note, and template are available from the Information Governance Team or via the staff intranet site.

7.0 Training

The Data Security Awareness Level one course is mandated for everyone working in health and care. It has been designed to inform, educate and upskill staff in data protection, data security and information sharing. It provides an understanding of the principles and importance of data security and information governance. It looks at staff responsibilities when sharing information and includes a section on how to take action to reduce the risk of breaches and incident. Staff can access the course via the LMS system.

8.0 Compliance with this policy

8.1 Article 5(1) of the UK GDPR states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Therefore, NSCHT has a legal obligation to:

a) Identify a 'lawful basis' for collecting and using personal data.

b) Ensure data is processed in a way that is not detrimental, unexpected or misleading to the individuals concerned.

c) Ensure NSCHT tells people about data processing to be open and honest before their data is used.

8.2 Staff compliance with this policy

Any breach of, or refusal to comply with this policy may lead to disciplinary action in accordance with relevant trust policies and procedures. In serious cases, a breach may be regarded as gross misconduct and may result in dismissal.

Individuals may be personally charged under criminal or civil law, and prosecuted for breaches of confidentiality, which are caused by malice or negligence.

Section 170(1) of the Data Protection Act 2018 states that it is an offence for a person knowingly or recklessly:

- to obtain or disclose personal data without the consent of the controller.
- to procure the disclosure of personal data to another person without the consent of the controller.
- after obtaining personal data, to retain it without the consent of the the controller in relation to the personal data when it was obtained.

9.0 Information Governance Incidents

It is essential that all Information Governance/Data Protection incidents are reported. The Incident Reporting Policy and Procedure Document (Trust Policy ref 5.01) sets out how to report incidents and near misses.

Everyone is responsible for reporting information incidents such as information being illegitimately accessed, used, disclosed, altered, destroyed, and or stolen, resulting in impairment or loss as soon as possible directly through Ulysses.

10.0 Monitoring, amendments and document control

This policy is reviewed every 3 years as a minimum or more frequently, as required by NHS England, Department of Health (DoH), NHS Digital and the ICO, to ensure the sections still comply with the current legal requirements and professional best practice, to provide value to the policy.

11.0 Legal considerations

NSCHT regards all identifiable personal information relating to patients as confidential and will undertake or commission annual assessments and audits of its compliance with legal requirements. The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

The Trust has established and will maintain policies to ensure compliance with Privacy and Data Protection Legislation, the Common Law Duty of Confidentiality and the NHS Code of Practice.

The Trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.

Failure to comply with the data protection regulations could result in reputational damage to the Trust and may carry financial penalties imposed by the ICO, or other regulatory action.

Under the Network and Information Systems Regulations 2018 (NIS Regulations) and UK GDPR, there are two tiers of administrative fine that can be imposed:

- The maximum fine for the first tier (breach of process) is £9.5 million or in the case of an undertaking up to 2% of total annual global turnover (not profit) of the preceding financial year, whichever is greater.

- The maximum fine for the second tier (serious data breaches) is £17.5 million or in the case of an undertaking up to 4% of total annual global turnover (not profit) for the preceding financial year, whichever is greater.

- The fines within each tier relate to specific articles within the Regulation that the organisation has breached.

Appendix One: Version Control

Version Number	Purpose/Amendment	Author	Date Changed
1.0	New Policy Created – applicable for North Staffordshire Combined Healthcare NHS Trust and associated GP Practices		21/02/2022