NHS
Cumbria, Northumberland, Tyne and Wear
NHS Foundation Trust

Document Title	Confidentiality Policy Protecting and Using Personal Information
Reference Number	CNTW(O)29
Lead Officer	Medical Director
Author	Angela Faill Head of Information Governance and Medico Legal
Ratified By:	Business Delivery Group
Date ratified	Sept 2021
Implementation date	Sept 2021
Date of full implementation	Sept 2021
Review Date	Sept 2024
Version	V04

Review and Amendment Log	Version	Type of change	Date	Description of change

This policy supersedes:

Reference Number	Title
CNTW(O)29 – V03.1	Confidentiality Policy

Confidentiality Policy

Standard Appendices attached to policy		
Appendix A	Equality Analysis Screening Tool	16
Appendix B	Training checklist and Needs Analysis	18
Appendix C	Monitoring / Audit Tool	20
Appendix D	Policy Notification Record Sheet **-** click here	

Appendices to be listed separately	
Document No:	**Description**
Appendix 1	The Data Protection Act Principles
Appendix 2	The Caldicott Principles
Appendix 3	Guidelines for Clinical Communications

Practice Guidance Note(s)	
PGN No:	**Description**
CP-PGN-01	Carer's Charter – Common Sense Approach to Sharing information with Carers

1 INTRODUCTION

1.1 Staff within Cumbria Northumberland, Tyne and Wear NHS Foundation Trust (the Trust/CNTW), have access to a great deal of very sensitive and highly confidential personal information on a daily basis. The information is often patient specific and may include personal health details or other personal matters. The confidentiality of this information must be respected and maintained at all times. Everyone therefore is required to act in such a manner as to uphold the principle of confidentiality.

2 PURPOSE

2.1 This policy will ensure that confidentiality is safeguarded and that all staff are aware of their responsibilities. The importance of this principle will be reinforced by inclusion in all job descriptions, Trust and departmental training, induction programmes, and contracts of employment.

2.2 The policy applies to all Trust staff, external NHS staff and individuals from Non-NHS bodies who are engaged in any capacity in Trust business where they receive, record, and store or otherwise come across personal information. The following must be adhered to:

2.3 The Common Law Duty of Confidentiality

- This means that information given in confidence must not be disclosed without a person's consent unless there is a valid justifiable reason such as a requirement of legislation being met, a Court order or it is judged that there is an overriding public interest to do so.

2.4 The Data Protection Act 2018

- The Data Protection Act puts strict controls on the use of personal information. Personal data is classed as information that can identify a living individual. It covers all computerised and paper records and covers all forms of personal information that is recorded i.e. X-rays, CCTV and photographic images. It has built upon the Data Protection Act 1998 in respect of concepts of personal data, data controller responsibilities/obligations, enhancing existing data subject rights. Essentially, the Data Protection Bill has made 'best practice' a legal requirement.
  The Act's six principles are shown in Appendix 1 of this policy.

2.5 The Caldicott Report and Reviews

- In 1996-7 Dame Fiona Caldicott chaired a review on the use of patient identifiable data where six principles were recommended for the protection of people's confidentiality, which became known as the 'Caldicott principles'. In 2013, she led the Information Governance Review where an additional 'Caldicott principle' was recommended. The revised Caldicott Principles can be found in Appendix 2 of this policy.

- In July 2016, a further review was undertaken which focused on cyber security, consent and 'opt-outs'. The aim of this review was to improve the use of data in people's interests and ensure transparency for the public about when their data will be used and when they can opt out of such usage.

2.6 Professional Codes of Conduct

- All health professionals must adhere to their professional codes of conduct, which reinforces the responsibilities in respect of service user confidentiality.

- Various guidance produced by these organisations, i.e. General Medical Council, advises on circumstances relating to appropriate sharing within a legislative framework.

2.7 Human Rights Act 1998

- In the UK, Human Rights are protected by this Act. One of these is the right to respect for family and private life, home and correspondence under Article 8. If personal information is disclosed to other people without consent, this can be an example of a breach of this right. Public bodies have to make sure their activities comply with the stated rights.

2.8 NHS Code of Practice: Confidentiality

- This Department of Health publication gives NHS staff detailed guidance on rules and legislation governing the use and disclosure of patient information. It also includes a number of flow charts, which CNTW have adopted to assist staff to make decisions on confidentiality and disclosures.

2.9 The Health and Social Care Act 2001 (section 60)

- Section 60 gives the Secretary of State Powers to permit the use of patient data in certain special cases without the necessity of gaining consent. A recent example of these powers has been to allow disclosure of patient data to support activities for cancer registries. Requests by persons or agencies who wish to gain access to patient data without obtaining consent will need to apply to the Patient Information Advisory Group (PIAG) who can advise the Secretary of State on such matters. This may affect researchers wishing to use Trust patient data.

2.10 Freedom of Information Act 2000

- The Act, which came into full effect January 2005, means that the majority of recorded information held by the Trust will be accessible to anyone. Documents this may affect include accounts, reports, policies, procedures and certain minutes of meetings. Where information that has been requested contains personal information, disclosure of those details will only be permitted if data protection conditions are met.

2.11 Public Interest Disclosure Act 1998 ("Whistle blowing")

- This Act gives employees certain legal protection against dismissal or being penalised by their employer where they disclose information, which may show malpractice within their organisation. Staff should consult the Trust's policy, CNTW(HR)06 Raising Concerns Policy, before considering any such disclosure to ensure they are aware of the mechanisms governing this internal procedure.

2.12 Information Governance (IG)

- Information Governance is the way by which the NHS handles information about patients, employees and members of the public. In particular where the Trust holds information that identifies an individual and/or relates to their health or other sensitive personal confidential data.

- There is an Information Governance Assurance framework for Health and Social care which sets out the activities and roles which individually and collectively ensure that information governance standards are clearly defined and met. It comprises a number of internal measures and organisational structures to improve information governance and external methods of providing oversight, monitoring and audit

- To achieve this the Trust completes an annual Data Security and Protection Toolkit (DSPT) submission. This Toolkit involves NHS organisations carrying out self-assessments of their compliance against the IG assertions which are taken from the National Data Guardian Data Security Standards.

- The National Data Guardian Data Security Standards have 3 leadership obligations which are:

    - People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.
    - Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
    - Technology: ensure technology is secure and up to date.

- The Information Governance assurance framework also covers the following:

  - The Data Protection Act 2018.
  - Caldicott Report and Reviews.
  - Records Management.
  - The Freedom of Information Act 2000.
  - Data accreditation and data quality.
  - Cyber Security and Risk Mitigation.

2.13 **Mental Capacity Act 2005**

- This Act makes provision for decisions to be made on behalf of individuals who lack capacity to make decisions for themselves. It includes statutory tests of capacity, best interests and makes provision for individuals to appoint someone of their choice as 'Lasting Power of Attorney' (LPA) to make financial and/or personal welfare decisions on their behalf when they lose capacity to do so themselves. This can include decisions about the use/sharing of personal information.

Breaches of the above may lead to disciplinary action for staff or the imposition of heavy fines on the Trust. A health professional can be struck off if they break their professional code of conduct.

A breach of confidentiality has the potential to damage both the reputation and credibility of the Trust.

3 DUTIES AND RESPONSIBILITIES

3.1 The Chief Executive on behalf of the Trust retains ultimate accountability for the health, safety and welfare of all service users, carers, staff and visitors; however key tasks and responsibilities will be delegated to individuals in accordance with the content of this policy

3.2 The Caldicott Guardian is the Trust's Executive Medical Director and is responsible for protecting the confidentiality of service user information and enabling appropriate information sharing. This includes the confidentiality of service user information held in the electronic health records. The Caldicott Guardian retains ultimate accountability for decision making for any Caldicott issues, and in particular for those that may have a major impact on the organisation.

3.3 The Caldicott Guardian is supported in their role by Deputy Caldicott Guardian and the Head of Information Governance & Medico Legal.

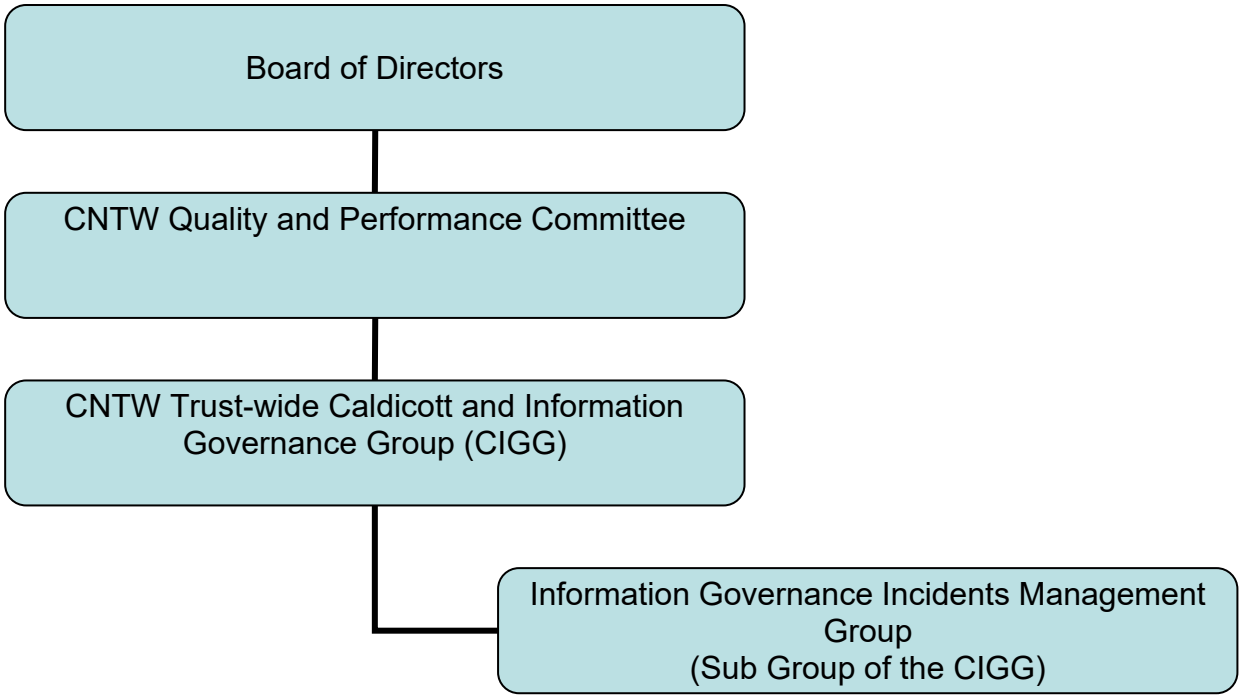
3.4 The Data Protection Officer (DPO), including Deputy DPO, is an independent role within the organisation and is responsible for ensuring that the controller, processor and employees who process personal data understand their obligations and providing advice on meeting those obligations. This role lies with the Head of Information Governance & Medico Legal.

3.5 The Senior Information Risk Owner (SIRO) is the Trust's Executive Director of Performance and Assurance and is responsible for identifying and managing information risks to the organisation. This includes oversight of the information security incidents and responses.

3.6 The SIRO is supported in their role by information asset owners who have assigned responsibility for the Trust information assets.

3.7 Directors and all managers at all levels are responsible for ensuring the policy and relevant practice guidance is applied consistently and appropriately in their area of responsibility.

3.8 The Trust corporate governance arrangements relevant to this policy are shown in the diagram below.



3.9 The Trust-wide Caldicott and Information Governance Group (CIGG) is responsible for ensuring that effective Information Governance and Caldicott best practice mechanisms are in place within the Group.

3.10 All staff at all levels in the Trust:

- Must be aware and fully understand their legal obligation to keep personal information which is obtained through their work confidential.
- Participate in induction, training and awareness raising sessions carried out to inform/update staff on confidentiality issues.
- To be aware of the Data Protection Officer in the Trust whom they should liaise with in respect of confidentiality issues.

- To challenge and verify where necessary the identity of any person who is making a request for confidential information and to determine the validity of their reason for requiring that information.
- To report any actual or suspected breaches of confidentiality to their line manager and to the Information Governance department at the earliest opportunity.
- To participate in audits/reviews of working practices to identify areas of improvement with regard to patient confidentiality and to implement any measures identified
- To ensure data is recorded accurately and contemporaneously in a legible manner and signed clearly in accordance with the Trust's CNTW(O)09 – Records Management Policy, practice guidance note (PGN) - RM-PGN-02 - Record Keeping Standards.

4 DEFINITION OF TERMS

Cumbria Northumberland, Tyne and Wear NHS Foundation Trust	The Trust/ CNTW
Patient Information Advisory Group	PIAG
Caldicott and Information Governance Group	CIGG
Information Governance	IG
Lasting Power of Attorney	LPA
Practice Guidance Note	PGN

5 USE AND DISCLOSURE OF PERSONAL INFORMATION

5.1 Service User Information

5.1.1 The use and disclosure of service user health information can only be undertaken when certain legal grounds are met. The essential conditions within the NHS environment are:

- Where the service user has provided information for their health care and treatment (this can include the management and administration processes that are necessary in order to provide that care and treatment). Where possible, they should be made aware of how their information is used and whom it may be disclosed to (see Section 6).
- Where there is an overriding public interest, a current and imminent risk of serious harm to the service user and/or others, an obligation in Law or a Court Order. Where appropriate, the service user should be made aware that information has been used or disclosed on this basis, unless to do so is likely to cause harm.
- The service user has given their explicit consent to the information sharing for purposes other than direct care and treatment.

5.1.2 Only persons who are directly involved in the care and treatment of the service user have a legal right to view the information and can have access. The information must be used for the purpose of providing direct care and treatment, or within the scope of consent provided only.

5.1.3 In all cases or using or disclosing information, the minimum necessary information should be disclosed and accessed. Where possible, the information should be completely anonymised

5.1.4 Under the Mental Capacity Act 2005, service users should be assumed to have capacity to make decisions about how their information is used or disclosed, unless it is established that they lack capacity under the statutory test in the Act. A service user should not be treated as unable to make their own decision about a specific issue unless all practicable steps to help them to do so have been taken without success. If a service user's capacity is fluctuating, the clinical team may wait until a time that the service user regains capacity. Further guidance around applying the MCA 2005 can be found in CNTW(C)34, the Trust's Mental Capacity Act 2005 Policy and associated PGNs: https://www.cntw.nhs.uk/about/policies/mental-capacity-act-2005/.

5.1.5 Service users can appoint someone of their choice via a Lasting Power of Attorney document to make personal welfare decisions for them, including decisions about how their information is used or shared. If the service user lacks capacity and an LPA is in place, the person with LPA should be given the information set out in Section 5 and should be asked for their consent to the use/disclosure of the service user's information.

5.1.6 If there is no LPA in place, decisions on the use or sharing of information must be made by the clinical team in the incapable service user's best interests. The Mental Capacity Act 2005 provides a statutory best interests' test.

5.1.7 In cases of disagreement between the person with LPA and the clinical team, for example where the person with an LPA is agreeing to limited access only and the team do not believe this to be in the service user's best interests, the Caldicott Guardian should be consulted. If necessary, the Court of Protection may be involved to settle a dispute.

5.1.8 Where service user information (which has not been completely anonymised) is being considered for other uses such as research or education this will always require consent of the service user to use it in this way.

5.2 Use of Special Categories of Personal Data (previously personal sensitive)

5.2.1 The Data Protection Act 2018 classes certain information as special category, this is where it contains details of a person's:

- Criminal record.
- Health information.
- Political views.
- Racial origin.
- Sexual life.

- Trade Union membership.
- Religious beliefs.
- Genetic and Biometric data.

5.2.2 Where a Trust use this type of information, they must be certain they have a justifiable reason to do so (as detailed in the Data Protection Act).

5.3 Non-sensitive Personal Data

5.3.1 Non-sensitive personal data such as name, address, date of birth etc. will also be used in many departments. Although the conditions for use and disclosure of this kind of information are not as stringent as for special categories of data, its collection and use will still have to be justified. An example of this is finance staff needing certain personal details in order to pay staff that in turn will contribute directly or indirectly to the organisation's healthcare process.

6 INFORMING PEOPLE ON THE USE OF THEIR INFORMATION

6.1 The Data Protection Act 2018 states that individuals have to be provided with information where organisations or person(s) hold and use their personal information, the information to be provided must include:

- The purposes for which it is being used.
- The likely disclosures of their information.
- The likely consequences of the processing.
- Any other information that is necessary.

6.2 The Trust has a Fair Processing Notice which is available on the Trust Internet. This can be accessed by clicking on the following link: https://www.cntw.nhs.uk/foi/data-protection/

6.3 For service users, information should ideally be given by clinicians and leaflets made available to further complement this requirement:

- Information the Trust Holds About You.

- Common Sense Confidentiality.

6.4 Providing advice and responding to individuals about the use of their information

6.4.1 There may be occasions where the Trust is considering using an individual's personal information for another purpose or disclosing it to a person or organisation that the individual(s) would not have anticipated. In which case, the Trust may need to make arrangements to inform individuals about these new uses of their information. This may also necessitate future updates of service user leaflets or fair processing notices which explain how service user health records are used. Service users and other individuals may also contact the Trust about a number of issues related to use of their personal information, this may include:

- Objections to how their personal information is processed.
- Requests for certain possible disclosures of their information to be restricted.
- Requests for detailed information about how their information is used by the Trust.

6.4.2 If you have received communications such as these or are considering new uses or disclosures of individuals' personal records, you will need to contact the Information Governance & Medico and Legal Department (contact details on page 13) to ensure satisfactory responses and actions are taken.

7 INFORMATION SHARING WITH OTHER AGENCIES

7.1 It may be necessary for essential personal/personal sensitive information to pass between the NHS, Local Authority, Social Services and other services. This may happen, for example, where one of these services is contributing towards a programme of care. Where information is shared, it may be necessary for an information sharing agreement to be in place. This will give the Trust necessary guarantees on the security of the information.

7.2 All personal information that is used in the information sharing agreement must meet the conditions for processing as laid down in the Data Protection Act 2018. Where that personal information also has a duty of confidence and it is to be shared for a different purpose to that for which it was given, it should only be disclosed if one of the following requirements has been met:

- The individual has given their consent
- The disclosure is a requirement of a statute of law; or
- There is an overriding public interest in making the disclosure.

7.3 An Information Sharing Agreement should be in place to outline an agreed approach to the information sharing. It may be that these arrangements are made clear in other documents such as a Service Level Agreement or contract. The document should outline the legal grounds for information sharing as well as the practicalities of this i.e. what information is shared, how this is shared, when is this shared, why is this shared, to whom is this shared etc. An Information Sharing Agreement is **not** a legal authority in itself.

7.4 It must be appreciated, however, there may be occasions where confidentiality is not absolute and it could be essential that it be breached. This may be appropriate where it becomes necessary to protect an individual from harm such as in a child protection case or personal/special categories of personal data is required for a serious crime investigation. Also, Law might allow a disclosure without consent, for example Public Health legislation stipulates that designated NHS staff need to notify the relevant authority where a person is suspected of contracting a notifiable disease.

7.5 Where information would be disclosed without or against the consent of the individual, or the person with Lasting Power of Attorney for an incapacitated

patient, the decision to release information and any support that is required can be referred to the Information Governance & Medico Legal Department and as appropriate, the Caldicott Guardian. An example of this is where the information is required under a court order, statute or there is an overriding public interest for doing so. It may be appropriate for this person to seek additional legal or specialist advice if information is to be disclosed without the individual's consent.

7.6 A formal record, for example via a clinical entry, must be kept by the relevant agency as to the reason why a disclosure of personal information was made. Where public interest is the reason, the grounds for doing so should be clearly documented to reason for the request, decision making, advice sought and outcome.

7.7 Each case should be judged on its merits whether a disclosure without consent is justified. Decisions must be made by those involved with direct care and treatment and/or where necessary the Trust's Caldicott Guardian. Where clinicians require support in respect of decision making, they can seek support from the Information Governance & Medico Legal Department and as appropriate, the Caldicott Guardian.

7.8 Information, which has been aggregated or anonymised, can generally be shared for justified purposes. Care should be taken to ensure that individuals cannot be identified from this type of information, as it is possible to identify individuals from limited information through triangulation of data. If individuals can be identified by the information, normal legislative requirements would then apply. In all cases only the minimum identifiable information necessary to satisfy the purpose should be made available.

7.9 An individual has a right to request that information about them be withheld from someone or some agency, which might otherwise have received it. The individual's wishes should be respected unless there are exceptional circumstances.

7.10 For further guidance, please refer to the 'To Share or Not to Share' flowchart within the Information Sharing policy: CNTW(O)62 - Appendix 3.

8 DISCLOSURE OF PERSONAL/SPECIAL CATEGORIES OF DATA TO THE POLICE

8.1 Where the Trust receives a request for personal/special categories of data from the police, certain information can be released if legislation dictates the need for disclosure:

- The Police have provided informed and explicit consent from the individual.
- The information is required in the prevention, detection and prosecution of a serious crime, i.e. murder, rape.
- The information is required under the Road Traffic Act.
- The police have produced a Court order.

8.2 Any request by the Police should be in writing stating what information they require, why they require it and under what legal authority (see above) they are requesting it. The Trust will require sight of any legal authority cited. The Disclosure Team will co-ordinate this request.

8.3 The Crime and Disorder Act 1998 gives NHS organisations the power to share information with the Police for the purposes of the Act. Additionally, the Trust may consider a disclosure is necessary in the overriding public interest. This could be, for example, to provide information which will assist the police in solving a serious crime such as a murder or rape case.

8.4 In all cases, a decision to release information is made by those with the appropriate authority i.e. the current or most recent healthcare professional or Caldicott Guardian.

9 SECURITY OF INFORMATION

9.1 All records containing personal information, whether they are kept in files or stored on PC's, laptops or any other form of electronic capture device, must be secure. This can be achieved by following the guidance in the Information Security Policy, CNTW(O)35. Below are some basic rules on maintaining the confidentiality of personal information.

9.2 Manual records

9.2.1 They should be stored securely in locked rooms or cabinets. Confidential information, such as service users' records, must not be left lying around in accessible areas such as reception desks where members of the public or unauthorised staff may view them.

9.3 Electronic records

9.3.1 All Trust PCs and laptops are encrypted and are accessible via unique logins and passwords. Access to electronic records stored in the Patient/Staff information systems will also have unique logins and passwords. Passwords must not be shared.

9.3.2 When not in use, PCs or laptops should be switched off or have a secure screen saver in use. Laptops/handheld devices are to be kept secure in locked rooms or cabinets or in a safe environment (where members of staff are present at all times).

9.3.3 Trust information is not to be stored on personal devices unless the Trust's Digital service desk has approved the access using the agreed application.

9.4 Telephone enquiries

9.4.1 When telephone enquiries are received asking for disclosure of personal information, the caller should be asked to put their requests in writing enclosing the appropriate authority where applicable. Where requests have to be dealt with urgently, the following rules must be adhered to:

- The disclosure is legally justified and the caller has a legal right to access that information.
- You are certain the caller is who they say they are; you can confirm this by carrying the following checks:
    - Verify personal details.
    - If the caller is part of an organisation/company, you should obtain the main switchboard number of that organisation (via phone book or directory enquires) and ring back.
- Always provide the minimum amount of information that is necessary.
- If in doubt, tell the caller you will ring back. Where necessary, consult a senior manager or the designated authority for confidentiality issues within the Trust.

9.5 **Answer phones**

9.5.1 You must only leave a message on a service user's or individual's answer phone if it is urgent. If this is the case, leave your name and number only – do not identify where you are calling from or provide any identifiable service user details.

9.6 **Transfer of Records**

9.6.1 Every care should be taken transferring records that contain personal information both internally and externally, ensuring that envelopes are addressed correctly (addresses should include a named person and title, department and location) and be clearly marked "private and confidential".

9.6.2 Transfer of personal information should only be made via the Internet if the means of transfer is regarded as being secure and has been authorised as such by an appropriate authority. Clinical communications between NHS organisations can be made over NHSmail – guidelines were agreed by the British Medical Association and the NHS Information Authority (see Appendix 3). Please check with the appropriate person first, i.e. Information Governance, Caldicott Guardian or Line Manager. Please also refer to the Trust's CNTW(O)44 – Acceptable Use of Email Policy and CNTW(O)65 – Acceptable Use of Intranet and Internet Policy.

9.7 **Data Protection Contracts**

9.7.1 Where another organisation carries out duties (such as a computer maintenance company or temporary nurse arrangement) on behalf of the Trust which involves them having access to personal data, a contract and confidentiality agreements should be made which gives the Trust sufficient guarantees in respect of the confidentiality of that information.

9.8 **Conversations or Accessing Information in Public**

9.8.1 Where conversations are conducted by staff relating to Trust business, or information is accessed i.e. via Trust devices, this should only be done in an appropriate environment where the content of information cannot heard or

seen by those who do not have a right to have this information. This can also apply where recorded messages are replayed.

9.8.2 Where there are concerns around maintaining confidentiality in environments i.e. meeting rooms or offices, this should be raised with management as a matter of urgency to ensure procedures are implemented to improve the situation. Where support is needed, contact can be made with the Information Governance & Medico Legal Department.

10 REPORTING A BREACH OF CONFIDENTIALITY/MISUSE OF PERSONAL DATA

10.1 Any breach of confidentiality or misuse of personal information must be reported via the Trust's policy, CNTW(O)05 Incident Policy (Including the Management of Serious Incidents).

10.2 To report an IG incident, please use the Trust's web-based reporting system, available by clicking here.

10.3 The Quality & Performance Committee receive a regular assurance report in relation to IG activity including incidents. The Information Governance & Medico Legal Department review all IG-reported incidents, escalating appropriately to the IG Incidents Group for review and appropriate action.

11 CONTACTS FOR CONFIDENTIALITY ISSUES

- Disclosures/Medico Legal Team
  Information Governance & Medico Legal Department
  St Nicholas Hospital
  Jubilee Road
  Gosforth
  Newcastle
  NE3 3XT
  Tel: (0191) 2466896/ (0191) 2466891
  E-mail: disclosures@cntw.nhs.uk
  DPO@cntw.nhs.uk

- Data Protection Officer/Deputy DPO- Angela Faill
  Information Governance & Medico Legal Department
  St Nicholas Hospital
  Jubilee Road
  Gosforth
  Newcastle
  NE3 3XT
  Tel: 0191 2466896
  E-mail: DPO@cntw.nhs.uk

- The Caldicott Guardian and Deputy Caldicott Guardian can be contacted via: Caldicott@cntw.nhs.uk

12 IDENTIFICATION OF STAKEHOLDERS

12.1 This is an existing Policy with no changed content that relates to operational and / or clinical practice and thus Trust-wide consultation was not required.

- North Locality Care Group
- Central Locality Care Group
- South Locality Care Group
- North Cumbria Locality Care Group
- Corporate Decision Team
- Business Delivery Group
- Safer Care Group
- Communications, Finance, Digital Services
- Commissioning and Quality Assurance
- Workforce and Organisational Development
- NTW Solutions
- Local Negotiating Committee
- Medical Directorate
- Staff Side
- Internal Audit
- Safety, Security and Resilience

13 TRAINING

13.1 Training for this Policy is incorporated into the annual Information Governance Training mandated to all staff.

13.2 Where additional training is required, it is the responsibility of both managers and staff to ensure that this is undertaken and that attendance is verified and recorded.

14 IMPLEMENTATION

14.1 Taking into consideration all the implications associated with this Policy, it is considered that a target date of September 2021 is achievable for the contents to be implemented across the Trust.

15 FAIR BLAME

15.1 The Trust is committed to developing an open learning culture. It has endorsed the view that, wherever possible, disciplinary action will not be taken against members of staff who report near misses and adverse incidents, although there may be clearly defined occasions where disciplinary action will be taken.

16 FRAUD, BRIBERY AND CORRUPTION

16.1 In accordance with the Trust's Policy CNTW(O) 23 – Fraud, Bribery and Corruption Policy and Response Plan, all suspected cases of fraud and

corruption should be reported immediately to the Trust's Local Counter Fraud Specialist or to the Executive Director of Finance.

17 MONITORING COMPLIANCE

17.1 Responsibility for monitoring compliance with this Policy locally lies with Associate Directors and Line Managers.

17.2 The Information Governance Team will monitor compliance with this Policy through observation, spot checks and through incident management in line with the Trust Incident reporting process.

17.3 Any compliance issues will be reported to the Line Managers concerned and may be handled through staff disciplinary processes or contractual arrangements.

17.4 Incident Reporting

17.4.1 All incidents involving the loss of data whether encrypted or unencrypted must be reported immediately to the Information Governance Department and dealt with in accordance with the Trust Incident Reporting Procedure (See Trust Policy CNTW(O)05 - Incident Reporting and Procedures).

17.4.2 To report an IG incident, please use the Trust's web-based reporting system, available by clicking here.

18 ASSOCIATED DOCUMENTATION

- CNTW(O)01 – Development and Management of Procedural Documents
- CNTW(O)05 – Incident Policy (IP-PGN-11)
- CNTW(O)09 – Records Management (and associated PGNs)
- CNTW(O)28 – Information Governance Policy
- CNTW(O)35 – Information Security Policy
- CNTW(O)36 – Data Protection Policy
- CNTW(O)44 – Acceptable use of Email Policy
- CNTW(O)62 – Information Sharing Policy
- CNTW(O)65 – Acceptable use of Intranet and Internet Policy
- CNTW(HR)06 – Raising Concerns Policy

19 REFERENCES

- https://ico.org.uk/
- https://digital.nhs.uk/
- https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#conformance-statements
- https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/.
- https://www.gov.uk/government/organisations/national-data-guardian
- https://www.nhsx.nhs.uk/

Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust

Appendix A

Equality Analysis Screening Toolkit			
Names of Individuals involved in Review	**Date of Initial Screening**	**Review Date**	**Service Area / Locality**
C. Rowlands and A. Faill	Aug 2021	Sept 2024	Trust wide
Policy to be analysed		**Is this policy new or existing?**	
Confidentiality Policy – V03 **Protecting and Using Personal Information**		Existing	
What are the intended outcomes of this work? Include outline of objectives and function aims			
Staff within the Trust have access to a great deal of very sensitive and highly confidential personal information on a daily basis. The information is often patient specific and may include personal health details or other personal matters. The confidentiality of this information must be respected and maintained at all times. Everyone therefore is required to act in such a manner as to uphold the principle of confidentiality. This policy will ensure that confidentiality is safeguarded and that all staff are aware of their responsibilities. The importance of this principle will be reinforced by inclusion in all job descriptions, Trust and departmental training, induction programmes, and contracts of employment. The policy applies to all NHS staff including those from Non-NHS bodies who are engaged in any capacity in Trust business who receive, record, store or otherwise come across personal information. The following must be adhered to:			
Who will be affected? e.g. staff, service users, carers, wider public etc			
Staff			
Protected Characteristics under the Equality Act 2010. The following characteristics have protection under the Act and therefore require further analysis of the potential impact that the policy may have upon them			
Disability	BSL interpreters, information in accessible formats including easy read, issues around lasting power attorney		
Sex	Not applicable		
Race	Language barriers. Need for interpreter/leaflets in community languages to explain need for information		
Age	Ensuring where the divide between parental responsibility and when child is ‘Gillick Competent’ lies		
Gender reassignment (including transgender)	Not applicable		
Sexual orientation.	Not applicable		
Religion or belief	Not applicable		
Marriage and Civil Partnership	Not applicable		

Pregnancy and maternity	Not applicable
Carers	Not applicable

Other identified groups	
How have you engaged stakeholders in gathering evidence or testing the evidence available?	
Through policy process	
How have you engaged stakeholders in testing the policy or programme proposals?	
Through policy process	
For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:	
All stakeholders in the standard policy review process	
Summary of Analysis Considering the evidence and engagement activity you listed above, please summarise the impact of your work. Consider whether the evidence shows potential for differential impact, if so state whether adverse or positive and for which groups. How you will mitigate any negative impacts. How you will include certain protected groups in services or expand their participation in public life.	
Accessible formats to be provided for all information produced on the policy. Briefing for interpreters. Need to monitor the policy carefully during its implementation.	
Now consider and detail below how the proposals impact on elimination of discrimination, harassment and victimisation, advance the equality of opportunity and promote good relations between groups. Where there is evidence, address each protected characteristic	
Eliminate discrimination, harassment and victimisation	NA
Advance equality of opportunity	NA
Promote good relations between groups	NA
What is the overall impact?	NA
Addressing the impact on equalities	NA

From the outcome of this Screening, have negative impacts been identified for any protected characteristics as defined by the Equality Act 2010?

If yes, has a Full Impact Assessment been recommended? If not, why not?

Manager's signature: A Faill Date: Aug 2021

Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust

Appendix B

Communication and Training Check list for policies

Key Questions for the accountable committees designing, reviewing or agreeing a new Trust policy

Is this a new policy with new training requirements or a change to an existing policy?	Change to an existing policy
If it is a change to an existing policy are there changes to the existing model of training delivery? If yes specify below.	No
Are the awareness/training needs required to deliver the changes by law, national or local standards or best practice? Please give specific evidence that identifies the training need, e.g. National Guidance, CQC, NHS Solutions. Please identify the risks if training does not occur.	Ensure that all staff are made aware of Trust Policy, Legislation and national guidance,
Please specify which staff groups need to undertake this awareness/training. Please be specific. It may well be the case that certain groups will require different levels e.g. staff group A requires awareness and staff group B requires training.	Trust wide
Is there a staff group that should be prioritised for this training / awareness?	It is essential that all staff groups within the Trust are made aware of the policy and the responsibilities associated with the legislation and guidance.
Please outline how the training will be delivered. Include who will deliver it and by what method. The following may be useful to consider: Team brief/e bulletin of summary Management cascade Newsletter/leaflets/payslip attachment Focus groups for those concerned Local Induction Training Awareness sessions for those affected by the new policy Local demonstrations of techniques/equipment with reference documentation Staff Handbook Summary for easy reference Taught Session E Learning	Team brief, CEO Bulletin, Intranet, face to face training, E-learning ,Staff IT Handbook
Please identify a link person who will liaise with the training department to arrange details for the Trust Training Prospectus, Administration needs etc.	Head of Information Governance and Medico Legal.

Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust

Appendix B – continued

Training Needs Analysis

Staff/Professional Group	Type of training	Duration of Training	Frequency of Training
All staff	Mandatory IG training	Online	Annual

Should any advice be required, please contact:- 0191 245 6777 (internal 56777) Option 1

Appendix C

Monitoring Tool

Statement

The Trust is working towards effective clinical governance and governance systems. To demonstrate effective care delivery and compliance, policy authors are required to include how monitoring of this policy is linked to auditable standards/key performance indicators will be undertaken using this framework.

CNTW(O)29 – Confidentiality Policy			
Auditable Standard/Key Performance Indicators		**Frequency/Method/Person Responsible**	**Where results and any associated action plan will be reported to, implemented and monitored;** (this will usually be via the relevant governance group).
1	Breaches of confidentiality are reported	Quarterly information governance highlight report which includes all IG incidents and complaints by Information Governance Manager to the Trust-wide Caldicott and Information Governance Group (CIGG).	Trust-wide Caldicott and Information Governance Group (CIGG).
2.	Serious incidents (as set out in Trust incident policy) are investigated	Quarterly information governance highlight report which includes all IG incidents and complaints by Information Governance Manager to the Trust-wide Caldicott and Information Governance Group (CIGG).	Trust-wide Caldicott and Information Governance Group (CIGG).

The Author(s) of each policy is required to complete this monitoring template and ensure that these results are taken to the appropriate Quality and Performance Governance Group in line with the frequency set out.