<table>
<thead>
<tr>
<th>Document Title</th>
<th>Information Sharing Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Number</td>
<td>NTW(O)62</td>
</tr>
</tbody>
</table>
| Lead Officer | Lisa Quinn, Director of Performance and Assurance  
Dr Suresh Joseph, Medical Director (Caldicott Guardian) |
| Author(s) | Sue Proud  
Information Governance Manager  
Angela Faill  
Health Records /Caldicott Lead |
| Ratified by | Quality and Performance Committee |
| Date ratified | 22nd June 2010 |
| Implementation Date | Operational Policies: May 2010 |
| Date by which policy to be embedded | September 2010 |
| Review Date | June 2011 |
| Version number | V01 |
| Date | Version | Reason |
| March 2010 | V01 | Solicitors review |

This policy supersedes:

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
## Information Sharing Policy

<table>
<thead>
<tr>
<th>Section</th>
<th>Contents</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Purpose</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Responsibilities</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Consultation &amp; Communication with stakeholders</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>Approval of Document</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Information Sharing</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>Governance</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>Policy Administrative Process</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>Equality Impact assessment</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>Training</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>Embedding</td>
<td>15</td>
</tr>
<tr>
<td>12</td>
<td>Standards/Key Performance Indicators</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>Fair Blame</td>
<td>15</td>
</tr>
<tr>
<td>14</td>
<td>Associated documents</td>
<td>16</td>
</tr>
<tr>
<td>15</td>
<td>References</td>
<td>16</td>
</tr>
<tr>
<td>16</td>
<td>Glossary of Terms</td>
<td>16</td>
</tr>
</tbody>
</table>

### Appendices – attached to policy

<table>
<thead>
<tr>
<th>Appendices</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Sharing Agreement</td>
</tr>
<tr>
<td>2</td>
<td>Data Protection Act 1998 Principles</td>
</tr>
<tr>
<td>3</td>
<td>Caldicott Approval Form</td>
</tr>
<tr>
<td>A</td>
<td>Equality and Diversity Impact Assessment</td>
</tr>
<tr>
<td>B</td>
<td>Training Checklist and Training Needs Analysis</td>
</tr>
<tr>
<td>C</td>
<td>Audit Monitoring Tool</td>
</tr>
<tr>
<td>D</td>
<td>Policy Notification Record Sheet</td>
</tr>
</tbody>
</table>
1. **Introduction:**

1.1 This Information Sharing Policy has been developed for Northumberland, Tyne and Wear NHS Trust (NTW) but may be used by all public sector organisations in the North East and any other organisation that would benefit from this guidance in managing information sharing arrangements.

- This Information Sharing Policy comprises the common principles and procedures to be adopted.
- This Information Sharing Policy sets out the basis for agreement between agencies to govern the sharing of personal information about service users and facilitate the development of information sharing agreements.
- This Information Sharing Policy will be supplemented by the Information Sharing Agreement as attached at Appendix 1 and the Practice Guidance Note.
- Whilst personal information held by NHS Organisations should be properly protected, there is also a growing expectation that information will be shared between health bodies, public and local authorities and the police service where it is appropriate to do so. Sharing information is a key element in the delivery of high quality, cost effective and seamless public services.
- The Health Act 1999 has expanded the statutory obligations on public service agencies to work together in the planning and delivery of health and social care services. Implicit in performing this duty is the need to share information.
- The Data Protection Act 1998 places an emphasis on the protection of patient identifiable information which has, in the past, made agencies very reluctant to share information for fear of breaking the law. It also meant however, that information which should have been shared was kept within one agency. There is a need to share information within a framework of clear understanding between agencies.
- The Department of Health Guidance 'Information Sharing and Mental Health- Guidance to Support Information Sharing by Mental Health Service (DOH 2009) emphasises the importance of information sharing in order to deliver effective public services and to enable early intervention and protection where necessary.
• The Caldicott Guardian Manual 2006 recommended that policies should be developed to protect the exchange and disclosure of patient identifiable information.

• The Trust therefore recognises the importance of information sharing within a framework of appropriate controls to protect confidential and sensitive information.

2. Purpose

2.1 The purpose of this policy is to:

• Ensure common understanding exists between the agencies within the North East as to the importance of information sharing, confidentiality and information security.

• Set out the basis for the secure transfer and use of person identifiable information across traditional organisational boundaries.

• Provide a robust framework for the legal, secure and confidential sharing or joint processing of personal data.

• Define the key principles which will facilitate the sharing of personal data with partner organisations.

• Establish a common standard to which all partner organisations will aspire in respect of the treatment of personal data.

• Assist professionals to feel confident that personal information is being shared in the right ways for the right reasons.

2.2 This policy will:

• Set out the legal framework and basis for information sharing.

• Define the responsibilities of the organisation and individuals within the organisation for information security and sharing.

• Establish the key principles inherent in all aspects of information sharing.

• Establish the process for Data Flows and Caldicott Approval.

• Establish the use and format of the Information Sharing Agreement.
3. **Responsibilities:**

3.1 **The Trust:**

- Ensuring that staff, volunteers and contractors are provided with the necessary training to be aware of, and comply with, their responsibilities in regard to the confidentiality of information.

3.2 **Chief Executive:**

- Overall responsibility for implementation of and compliance with this Policy.

3.3 **Trust Senior Information Risk Owner (SIRO):**

- Coordinating development and maintenance of information risk management policies, procedures and standards for the Trust.
- The ongoing development and day to day management of the Trust's Information Risk Management Programme.

3.4 **Caldicott Guardian:**

- Overseeing the establishment of procedures governing access to, and the use of personal information and where appropriate, the transfer of that information to other bodies.
- Upholding the Caldicott principles, taking account of the codes of conduct provided by professional bodies.

3.5 **Caldicott and Health Records Lead and Information Governance Team:**

- Dealing with enquiries, providing advice and guidance to support the appropriate use of sharing personal information.
- Supporting the Caldicott Guardian and Senior Risk Owner (SIRO).
- Supporting staff in obtaining Caldicott approval for information sharing.

3.6 **Trustwide Records Management, Information Governance and Caldicott Group:**

- Developing and supporting the implementation of Information policies and procedures and supporting the appropriate sharing of information.
3.7 Operational Directors:

- Ensuring implementation throughout their respective Directorates.

3.8 Trust Information Asset Owners (IAOs):

- Ensuring that information risk assessments are performed routinely on all information assets where they have been assigned 'ownership' following guidance from the SIRO on assessment, method, format, content and frequency.
- Authorising/ controlling system administration.

3.9 Line Managers:

- Line managers are responsible for ensuring staff in their service area implement the requirements of this policy, including providing appropriate advice and support. Line managers should bring to the attention of the Trust Wide Records, Information Governance and Caldicott Group any issues related to information risk or policy implementation.

All Employees of the Trust, Temporary Staff, Volunteers, Contract and Agency Staff and any other persons working on behalf of the Trust are bound by this policy and should be aware that any breach of confidentiality could be a matter for disciplinary action.

4. Consultation and communication with stakeholders

4.1 This Policy has been developed in consultation with:

Senior Management Team
Working Age Adult Directorate
Forensic Directorate
Older People's Services Directorate
CYP and Specialist Services Directorate
Learning Disability Services Directorate
Clinical Governance and Nursing Directorate
Finance, Informatics, Estates and Performance
Medical Staff Committee
Staff-side
Trust Pharmacy
Workforce
Allied Health Professionals – Strategic Forum
Communications

5. **Approval of document**

5.1 After full consultation, this document has been approved and ratified by the Quality and Performance Committee.

6. **Information Sharing:**

6.1 **Legal Framework:**

It is important that practitioners are aware of the legal framework which governs the sharing of personal information.

6.1.1 **Administrative Law:**

A public authority derives its powers from statute and must not act out of or in excess of those powers. Any act that is in excess of its powers is said to be ultra vires and may be subject to Judicial Review.

There is no general statutory power to enable public authorities to disclose personal information. It is necessary to consider legislation that relates to the policy or service that the sharing of data supports. From this it will be able to determine if there are express powers to share data or whether these can be implied.

6.1.2 **The Data Protection Act 1998 (DPA):**

The DPA regulates the processing of person identifiable information. The DPA should not be used as a barrier to sharing information if lawfully permitted.

The DPA requires that the processing of information must comply with the eight Data Protection Principles (attached at Appendix 2) and be in accordance with the rights of the data subject.

The Data protection Act 1998 provides that information can be shared even where consent has not been obtained only in the following circumstances:

- For the prevention or detection of crime and failure to disclose would be prejudicial to those purposes.
- Apprehension or prosecution of offenders.
- Where required by Court Order, statute or rule of law.
6.1.3 The Human Rights Act 1998 (HRA):

The HRA gives effect to the principles conferred by the European Convention on Human Rights (ECHR). It is unlawful for any public authority to act inconsistently with any of the Convention rights.

Article 8 of the ECHR provides the right to respect for private and family life. This right can only be interfered with when it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

6.1.4 The Common Law Duty of Confidentiality:

- Medical records and information constitute confidential information.
- Confidential information cannot be disclosed to a third party without lawful authority. A breach of this duty of confidence may result in an entitlement to damages.
- The duty of confidentiality requires that unless there is a statutory requirement or other legal basis for disclosure, confidential information should only be used for the purpose for which the patient disclosed it.
- Exceptions to the duty of confidentiality include where information is already in the public domain, where consent is sought and received, where disclosure is required by statute or Court Order, or where the public interest in disclosure outweighs the public interest in maintaining confidentiality.

6.1.5 Caldicott Guidelines:

The Caldicott Report of 1997 found compliance with confidentiality and security across the NHS 'patchy'. Every NHS and social care organisation has subsequently been required to appoint a 'Caldicott Guardian', responsible for the way in which confidential information is managed.

In respect of every use of patient identifiable information, the Caldicott Principles require public authorities to:

- Justify the purpose for using confidential information.
- Only use confidential information when absolutely necessary.
• Use the minimum that is required.
• Ensure that access is on a need to know basis.
• Ensure that everyone understands their responsibilities.
• Understand and comply with the law.

6.1.6 National and local guidance:

Compliance with relevant government and professional guidance is also important in ensuring that information is managed appropriately. Importance guidance includes:

• NHS Confidentiality Code of Practice – Department of Health 2003
• NHS Information Governance – September 2007
• Information sharing and mental health – guidance to support information sharing by mental health services. Department of Health 2009
• NMC Confidentiality Guidance 2009
• GMC Confidentiality Guidance 2009

6.1.7 Summary of the legal framework:

In order to ascertain whether there is a legal basis for information sharing the following should be considered:

• Whether there is a power to carry out the function to which the information sharing relates.

• Whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.

• Whether the data sharing would be in accordance with the Data Protection Act 1998, in particular the Data Protection Principles.

• Whether the sharing of the data would breach any obligation of confidence.

• Whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim and unnecessary in a democratic society.
• Whether the Caldicott Principles are complied with in any sharing of information.

6.2 **Key Principles of Information Sharing:**

6.2.1 **Commitment to share personal data:**

• To recognise that multi-agency initiatives require a commitment to sharing personal information about service users in compliance with national guidance and legislation.

6.2.2 **Compliance with Legislation:**

• To ensure that personal information is only shared in accordance with statutory duties, including the requirements of the Data Protection Act 1998.

6.2.3 **Compliance with Caldicott Principles:**

• Caldicott approval is required for all new routine data flows and also all 'one off' or ad hoc requests for release of health, social care or other personal information where consent is not available or is refused. The Caldicott Approval Form can be found at **Appendix 3**.

6.2.4 **Confidentiality:**

• To recognise that information is considered to be confidential when it appears reasonable to assume that the provider of the information believed that this would be the case.

• To recognise the importance of the legal duty of confidentiality. Confidential information will not be disclosed without the consent of the person concerned, unless there are statutory grounds or an overriding public interest justification for doing so.

6.2.5 **Consent:**

• To recognise that informed consent is the central principal in the use of personal information.

• To obtain the consent of the service user to share personal information wherever possible.

• To make service users aware of any information which will be shared and the purposes for which it will be used

• To share information where consent is refused only in exceptional circumstances and where there are appropriate statutory or public
interest grounds for doing so
• To keep records of the efforts made to obtain consent and details of whether consent was obtained or refused
• Consideration must be given to the provisions of the Mental Capacity Act 2005 (MCA). ISP-PGN-01

6.2.6 Justification / Purpose for Sharing:
• To clearly define the purpose and justification for information sharing. To ensure that when sharing personal information only the minimum required for the purpose is shared.

6.2.7 Fairness and Transparency:
• To ensure that the public are informed of the purposes for processing their personal information and to whom it will be disclosed.

6.2.8 Information Standards:
• Personal information will only be disclosed where it is legally justified.
• Personal information will be anonymised/pseudonymised where appropriate.

6.2.9 Requesting Data:
In accordance with the Caldicott Principles, any request for data should include;
• The purpose for which the information is to be used.
• The data items needed i.e. name, diagnosis etc (only the minimum data required to undertake the task should be requested).
• If relevant, who the data may be shared with.
• The time period for which the data will be held.
• An assurance that the data will be kept in a secure environment e.g. that data will be kept in a password protected database.
• An assurance that access to the information will be restricted and that the staff who have access to the data understand their responsibility to keep the data secure.
• An assurance that the organisation is registered with the Information Commissioner to hold and use the data they are requesting.
6.2.10 Complaints Procedure:

- Procedures should be in place to address complaints relating to the disclosure of information.
- All complaints and issues relating to information sharing must be dealt with in accordance with the Comments, Suggestions, Compliments and Complaints Policy NTW(O)07.

6.3 Data Flows:

- A data flow is a transfer of data between the Trust and a third party on a recurring basis, i.e. not an ad hoc single request.
- All new routine data flows must be agreed by the Caldicott Guardian / SIRO.
- Consideration will be given as to whether it is appropriate to enter an Information Sharing Agreement for a particular flow.
- Data flows will be mapped on an annual basis.

6.4 Caldicott Approval:

6.4.1 Caldicott approval is required for all new routine data flows and also all ‘one off’ or ad hoc requests for release of health, social care or other personal information, where consent is not available or is refused.

6.4.2 When a request to share information is made the Health Records / Caldicott Lead will:

- Consider whether sufficient information has been provided by the requestor.
- Consider whether the anonymous or pseudonymised data could be used.
- Maintain a log of all requests and decisions.
- Report requests to the Trustwide Records Management Information Governance and Caldicott Group.

6.5 Information Sharing Agreement:

6.5.1 Where a request for information is a request for a routine data flow or where large amounts of information are to be regularly shared, Caldicott Approval should be sought for the parties to enter an Information Sharing Agreement.
6.5.2 An ISA template is attached to this policy at Appendix 1.

6.5.3 Each Individual Information Sharing Agreement (ISA) will set out the detailed arrangements relevant to that particular application. All individual Information Sharing Agreements will need to be fully compliant and consistent with this Policy.

6.5.4 The ISA is not contractually binding and information may be shared without an ISA but should be used where appropriate to set good practice standards.

6.5.5 The ISA will include details of:

- The parties to the Agreement
- What Information is to be shared
- For what purpose information is to be shared
- On what legal basis the information is to be shared
- How frequently information will be shared
- How information security will be maintained
- What methods of recording, holding, retaining and disposing of information will be used

6.6 Retention and Security of Shared Information:

- All agencies should put in place policies or procedures governing the secure storage of all personal information retained in their manual or electronic systems.

- All agencies will ensure that retention and disposal processes for personal information are agreed and adhered to in line with organisational requirements.

- All agencies will recognise the importance of restricting access to personal information and maintain standards for technical security to protect shared information during transfer and within partner organisations.

7. Governance:

7.1 Monitoring Compliance:

7.1.1 Operational Directors will to monitor compliance with this Policy, in conjunction with the Health Records/Caldicott Lead and Caldicott Guardian.

7.1.2 Responsibility for monitoring compliance locally lies with Line Managers.
7.1.3 The Information Governance Team will monitor compliance through observation, spot checks and through incident management in line with the Trust Incident reporting process.

7.1.4 Compliance will routinely monitored through internal and external audit.

7.1.5 Any compliance issues will be reported to the IAO’s concerned and may be handled through staff disciplinary processes or contractual arrangements.

7.2 Incident reporting:

7.2.1 All incidents involving information sharing must be reported immediately to the Information Governance department and dealt with in accordance with the Trust incident reporting procedure (See Trust Incident Reporting Policy and Procedures).

8. **Policy administrative process:**

8.1. The development, consultation and dissemination of this policy has been undertaken in accordance with the Policy for the Development and Management of Procedural Documents and in conjunction with the policy administration process.

8.2 It has been circulated within the Trust e-bulletin and is available on the Trust Intranet site and also from policy administration.

8.3 Archiving of this policy will be in accordance with the Policy for the Development and Management of Procedural Documents.

9. **Equality impact assessment:**

9.1 In conjunction with the Trust’s Equality and Diversity Officer this policy has undergone an Equality and Diversity Impact Assessment which has taken into account all human rights in relation to disability, ethnicity, age and gender. The Trust undertakes to improve the working experience of staff and to ensure everyone is treated in a fair and consistent manner.

10. **Training:**

10.1 The Quality and Performance Committee has:

- given full consideration to any training needs that have been identified during the development of a policy
- ensured that a full Trustwide training needs analysis has been undertaken.
- identified who this will effect
- what level of training is required
• how often training should be undertaken
• any resource implication.

10.2 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.

11. **Embedding:**

11.1 Taking into consideration all the implications associated with this policy, it is considered that a target date of June 2010 is achievable for the contents to be embedded within the organisation.

11.2 This will be monitored by the Quality and Performance Committee during the review process. If at any stage there is an indication that the target date cannot be met, then the Group will consider the implementation of an action plan.

12. **Standards / Key Performance Indicators:**

12.1 The standards in this Policy are based on the requirements of the National Information Governance Assurance program and controls set out in the Information Governance Toolkit.

12.2 The Policy upholds the Principles of the Data Protection Act 1998, and the Caldicott report (HSG 98(89), as well as guidance issued by the Information Commissioners Office.

13. **Fair Blame:**

13.1 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 undertaken.

14. **Associated documents:**

Data Protection Policy NTW(O)36
Confidentiality Policy NTW(O)29
Information Security Policy NTW(O)35
Management of Records Policy and associated PGN’s
Email Intranet and Internet Policy NTW(O)44
Removable Media Data Encryption Policy NTW(O)30
Visual Imaging and Audio Policy NTW(O)45
Risk Management Policy NTW(O)33 and associated PGN’s
Incident Policy NTW(O)05 and Procedures and associated PGN’s
Information Risk Policy NTW(O)05

15. References

http://www.connectingforhealth.nhs.uk/
www.ico.gov.uk

16. Glossary of Terms:
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 tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Personal information: Factual information or expressions of opinion which relate to a living individual who can be identified from that information or in conjunction with any other information coming into possession of the information holder. This also includes information gleaned from a professional opinion, which may rely on other information obtained.

Information Sharing Agreement: An over-arching framework for sharing information between the Trust and one or more other agencies. It is not contractually binding but is used to set good practice standards that the parties need to meet in order to fulfil any duty of care which exists in relation to the regular/routine sharing of personal information.

Anonymised information: Information that cannot identify an individual.

Pseudonymised information: Information that has had any data making the data personally identifiable replaced by another non-identifiable data e.g. the NHS number replaced with a random ID number.
**Access to records requests:** The process by which the Trust responds to patient/service users who are entitled to see their records.
Joint Agency Information Sharing Agreement

1. Context and Background

Whilst personal information held by NHS Organisations should be properly protected, there is also a growing expectation that information will be shared between health bodies, public and local authorities and the police service where it is appropriate to do so. Sharing information is a key element in the delivery of high quality, cost effective and seamless public services.

Northumberland, Tyne and Wear NHS Trust (NTW) works closely with many other agencies and service providers and the appropriate sharing of information is essential.

This Agreement provides a framework for specific information sharing between agencies who are working together to provide mental health services.

This Agreement is to be read in conjunction with the NTW Information Sharing Policy.

A Practice Guidance Note dealing with information sharing is also available for practitioners.

2. Parties

Northumberland Tyne and Wear NHS Foundation Trust. (Specify service / directorate)

*Insert Partner/Partners here*

3. Legal Framework

The Legal Framework for Information Sharing is set out in the Trust Information Sharing Policy.

Medical information about a service user is personal data and is confidential. As such, there are strict legal restrictions and requirements in terms of the processing or sharing of data.

Information may be shared between agencies where it is done so in accordance with the Common Law Duty of Confidentiality, relevant legislation (notably the Data Protection Act 1998 and Human Rights Act 1998) and the Caldicott Principles.
4. Standards for Information Sharing

The Parties agree:

4.1 To comply with legislation.

- The parties adopting this agreement recognise their individual obligations to comply with all relevant legislation regarding the sharing and retention of person identifiable information, including but not limited to the Data Protection Act 1998 and Human Rights Act 1998.

4.2 To maintain the duty of confidentiality.

- Personal information will be deemed to have been provided in confidence, where it appears reasonable to assume that the provider of the information believed that this would be the case.

- All agencies will respect the duty of confidence and will not disclose any personal information without express consent, unless there are statutory grounds or an overriding public interest justification to do so.

4.3 To obtain consent for disclosure.

- All agencies will obtain explicit consent at the earliest opportunity from the individual concerned to share their personal information.

- In seeking consent, the individual will be made aware of the nature of the information to be shared, who the information may be shared with and for what purposes, and any other relevant details including their right to withhold or withdraw consent.

- In the event that consent is withdrawn, no further information will be disclosed unless there are statutory grounds for doing so or other legal exemptions can be applied. The agency sharing the information will notify any other agencies concerned.

4.4 To address refusal to consent to disclose appropriately.

- Parties to this agreement will ensure that any disclosure made without the consent of the individual is lawful. The decision to disclose should be authorised by an appropriate senior person and documented (with reasons) in the individual’s records.

4.5 To disclose appropriately.

- Information should only be disclosed for the relevant agreed purpose.

- Information should only be disclosed to the relevant agreed parties.

- Information disclosed and reasons for disclosure should be clearly
documented.

- Any disclosure without consent on a public interest basis should be necessary and proportionate to the risk involved.

4.6 To establish secure methods of transporting, retaining and disposal of shared personal information.

- Parties to this agreement will put in place policies to govern the secure transportation and retention of shared personal information. Such policies should include arrangements in relation to:
  - Internal and external postal arrangements.
  - Verbal, face to face and telephone sharing of information
  - Use of fax, DX, email and electronic transfer.
  - Use of encrypted electrical devices.

- Parties will ensure the safe, secure and appropriate disposal of shared information.

4.7 To establish staff awareness and training.

- Parties to this agreement will ensure that their staff understand and are aware of their legal obligations and responsibilities in relation to the sharing of personal information.

- Parties will ensure that staff are provided with appropriate training to enable them to share information legally, comply with professional codes of practice and comply with local and national policies.

- Parties will ensure that staff are aware that inappropriate disclosure of confidential information may result in disciplinary action.

4.8 To establish a complaints procedure.

- Parties to this agreement will put in place appropriate measures or procedures for dealing with inappropriate use or unauthorised access to personal information whether intentional or inadvertent.

- To adhere to the key principles of information sharing as provided in the NTW Information Sharing Policy.
5. **Third party access to information**

- The Parties agree that no third party shall have access to any information shared. Any request by a third party to access information will be directed to the record holder and treated as a new request.

6. **Process for sharing information**

6.1 **What information is to be shared?**

List all the information/documentation that will be shared. Be as specific as possible. Examples may include:

- Clinical and nursing records
- Needs assessments and Care Plans
- Risk Formulations and Management Plans
- Concerns about service users and any significant changes in their circumstances
- Care Co-ordination Reviews
- Referrals to provider
- Risk assessments

6.2 **For what purpose is information to be shared?**

6.3 **On what legal basis is information to be shared?**

- Will consent of the individual always be obtained?
- What if the patient is incapable?
- What if consent is refused?

6.4 **How frequently will information be transferred?**

6.5 **How will information security be maintained?**
6.6 What methods will be established to record, hold and dispose of shared personal information?

7. Agreement

7.1 The parties below agree to the terms of this Information Sharing Agreement.

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Authorised Official</th>
<th>Name</th>
<th>Signatories</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Northumberland Tyne & Wear NHS Foundation Trust
Information Sharing Policy NTW(O)62
Data Protection Principles

1. Principles:

The Data Protection Act states that all data controllers must comply with the following Data Protection principles:

Compliance with the eight principles of the Data Protection Act 1998 is enforceable under the legislation.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -
   a) At least one of the conditions in Schedule 2 is met;
   b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level or protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Individuals Rights:

The Act gives rights to individuals in respect of personal data held about them by others, these are:
- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Rights in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened
Caldicott approval form for use or release of patient identifiable data

You must address the 6 Caldicott Principles when submitting this request for data.

Project title: ...........................................................................................................................................

Description of data (principle 2 and 3) ......................................................................................................
...................................................................................................................................................................
.......................................................................................................................................................................

Indicate which data items have been requested:
Forename ☐ Surname ☐ DoB ☐ Age ☐ Sex ☐ Address ☐ Post code ☐

Name of organisation receiving data

Person responsible for the released data – Name .....................................................................................
• Job Title ........................................................................................................................................
• Address ..........................................................................................................................................

Purpose for which data are to be used (principle 1) ..................................................................................
..................................................................................................................................................................
..................................................................................................................................................................
..................................................................................................................................................................

I confirm that the data will be held and used according to the conditions described below and that I have addressed the 6 Caldicott principles.

Name:..........................................................................................................
Title:..........................................................

Signature: ......................................................... Date:......................................................

Other supporting information e.g. Ethics approval, correspondence etc

The release of data as described above: approved / not approved

Caldicott guardian / deputy: .......................................................... Date:.......................
The data will be treated as confidential.
1. The data will be used only for the purposes described.
2. In the case of anonymised or confidential aggregated data, no attempt will be made to identify or contact individuals or organisations identified through these data.
3. The data may be disclosed to staff of the above organisation but only for the purposes described.
4. The data may not be disclosed to any third party.
5. The data will be stored in secure condition at all times whether held on computer medium or as a printed copy.
6. The organisation to which the data are released will maintain and comply with a Data Protection Registration which encompasses the data and data usage described.
7. The data will be destroyed when the work is completed: any printed copies will be destroyed, and files deleted from computer systems (including any copies held on backup or archive media).
8. All staff given access to the data will be made aware of these conditions (principle 5)

Caldicott principles

Principle 1 - Justify the purpose(s)
Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use patient-identifiable information unless it is absolutely necessary
Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

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

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

Principle 5 - Everyone with access to patient-identifiable information should be aware of their responsibilities
Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Understand and comply with the law
Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

Caldicott Guardian for Northumberland, Tyne and Wear NHS Foundation Trust
Dr Suresh Joseph
Caldicott Guardian
St Nicholas Hospital
Gosforth
Newcastle upon Tyne
NE3 3XT

Tel No: 0191 22 32733 Email: angela.faill@ntw.nhs.
## Equality and Diversity Impact Assessment Screening Tool

<table>
<thead>
<tr>
<th>Names of Individuals involved in Review</th>
<th>Date of Initial Screening</th>
<th>Review Date</th>
<th>Service Area / Directorate</th>
</tr>
</thead>
<tbody>
<tr>
<td>S Proud</td>
<td>March 2010</td>
<td>March 2011</td>
<td>Trustwide</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy or Service to be Assessed</th>
<th>Is this a new or existing Policy or Service?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Sharing Policy</td>
<td>New</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Describe the aims, objectives or purposes of the Policy or Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that Person Identifiable and confidential Data shared with partner organisations is dealt with in accordance with the Data Protection Act 1998 and Caldicott principles, and that all staff are made aware of their personal responsibilities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Are there any associated objectives of the Policy or Service? If so what are they?</th>
</tr>
</thead>
<tbody>
<tr>
<td>To ensure that NHS local and National Guidelines on Information Sharing are adhered to.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does the policy unlawfully discriminate against equality target groups?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does the policy promote equality of opportunity for equality target groups?</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Does the policy or service promote good relations between different groups within the community, based on mutual understanding and respect?</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>
### Equality and Diversity Impact Assessment Screening Tool

Which equality target groups of the population do you think will be affected by this policy or function?

<table>
<thead>
<tr>
<th>Equality Target Group</th>
<th>What positive and negative impacts do you think there may be for each equality target group(s)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black and Minority Ethnic People (including gypsy/travellers, refugees and asylum seekers) BME</td>
<td>N/A</td>
</tr>
<tr>
<td>Women and Men WM</td>
<td>N/A</td>
</tr>
<tr>
<td>People in Religious/Faith groups RF</td>
<td>N/A</td>
</tr>
<tr>
<td>Disabled People DP</td>
<td>N/A</td>
</tr>
<tr>
<td>Older People OP</td>
<td>N/A</td>
</tr>
<tr>
<td>Children C</td>
<td>N/A</td>
</tr>
<tr>
<td>Young People YP</td>
<td>N/A</td>
</tr>
<tr>
<td>Lesbian Gay Bisexual and Transgender People LGBT</td>
<td>N/A</td>
</tr>
<tr>
<td>People involved in the criminal justice system CJS</td>
<td>N/A</td>
</tr>
<tr>
<td>Staff S</td>
<td>N/A</td>
</tr>
<tr>
<td>Any other group(s) AOG</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Equality and Diversity Impact Assessment Screening Tool

#### Screening Tool Checklist: Summary Sheet

<table>
<thead>
<tr>
<th>Positive Impacts</th>
<th>Negative Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Additional Information and Evidence Required** N/A

**Recommendations** N/A

---

**From the outcome of the Screening, have negative impacts been identified for race or other equality groups?**

No

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

---

**Manager's signature: S Proud**  **Date: 23.03.10**

Should any advice be required in respect of answering the above questions contact:

Equality and Diversity Officer

01670 394 848
## Communication and Training check list

It is the responsibility of Domain/Governance Committees to ensure a full review of any training implications has been undertaken prior to the ratification.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the change in knowledge or skills required to achieve the differences that this policy has been designed to deliver for the organisation?</td>
<td>Awareness and Guidance concerning safe sharing of data with partner organisations</td>
</tr>
<tr>
<td>Are the communication/training needs required to deliver the changes necessary by law, by national/local standards?</td>
<td>Ensure that appropriate training and support are provided to assist staff in safe sharing of information.</td>
</tr>
<tr>
<td>If yes, define the requirement(s). What does the organisation actually have to do.</td>
<td></td>
</tr>
<tr>
<td>For which staff groups is the communication/training need required?</td>
<td>Trustwide</td>
</tr>
<tr>
<td>What levels of understanding are required e.g. awareness of policy, understanding of new responsibilities/skills?</td>
<td>It is essential that all staff groups working with confidential/personal data are made aware of the policy and the personal responsibilities associated with it.</td>
</tr>
<tr>
<td>What means of delivery would be most appropriate e.g. team briefs, management cascade, e-bulletin etc?</td>
<td>Team brief, CEO Bulletin, Intranet, face to face training, E learning</td>
</tr>
<tr>
<td>Who will be the person responsible for liaising with Communications and the Training and Development Departments?</td>
<td>Head of Information/Health records Caldicott Lead</td>
</tr>
<tr>
<td>Service Area</td>
<td>Staff / Professional Groups</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Trustwide</td>
<td>All staff sharing service user, staff or confidential information with partner agencies or other third parties</td>
</tr>
<tr>
<td>Trustwide</td>
<td>All</td>
</tr>
</tbody>
</table>
AUDIT/MONITORING TOOL

STATEMENT

The Trust will work towards effective clinical governance and governance systems. To demonstrate effective care delivery and compliance regular audits must be carried out. Policy authors are encouraged to attach audit tools to all policies. Audits will need to question the systems in place as outlined in the policy. It is suggested that between five and eight measurable standard statements be listed, which can then be audited in practice and across the Trust.

<table>
<thead>
<tr>
<th>POLICY NAME</th>
<th>STANDARD STATEMENT: Information Sharing Policy</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement 1</td>
<td>The Trust must ensure that detailed procedures notes are in place in respect of the sharing and disclosure of data.</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Statement 2</td>
<td>The Trust must ensure that all staff are aware of their responsibilities under the Data Protection Act 1998.</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Statement 3</td>
<td>The Trust must ensure that it complies with the eight principles of the DP Act 1998 and the six principles of the Caldicott Report</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Statement 4</td>
<td>Information Sharing Agreements o be set up for all routine data flows or where large amounts of information are to be regularly shared, to be fully compliant and consistent with this Policy.</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Statement 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement 6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement 7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement 8</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### POLICY NOTIFICATION RECORD SHEET

<table>
<thead>
<tr>
<th>Policy number</th>
<th>NTW(O) 62</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy title</td>
<td>Information Sharing Policy</td>
</tr>
<tr>
<td>Date issued</td>
<td></td>
</tr>
<tr>
<td>Date of implementation</td>
<td></td>
</tr>
<tr>
<td>Directorate/Service/Ward/Department</td>
<td></td>
</tr>
<tr>
<td>Received by</td>
<td></td>
</tr>
<tr>
<td>Date received</td>
<td></td>
</tr>
<tr>
<td>Date placed in policy file</td>
<td></td>
</tr>
</tbody>
</table>

**I have read the above policy and understand its contents:**

<table>
<thead>
<tr>
<th>Name (print)</th>
<th>Signature</th>
<th>Designation</th>
<th>Service/Ward/Dept.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This form is to be kept up to date at all times to act as a clear record that all relevant staff have received notification of the existence of the above policy, that they have read it and understood its contents. Form to be retained in the policy file in front of the policy specified.

Policies and policy index lists are available via Trust Intranet. Index lists are continually updated and current lists should be retained in the front of policy files.