NORTHUMBERLAND AND NORTH TYNESIDE'S SAFEGUARDING ADULTS BOARD

MULTI-AGENCY INFORMATION SHARING AGREEMENT

February 2019

Foreword

Northumberland and North Tyneside's Safeguarding Adults Board is a multi- agency partnership responsible for co-ordinating the implementation of the Care Act 2014 and its guidance in relation to the development and implementation of policies and procedures to protect adults with care and support needs at risk from abuse or neglect.

The purpose of this document is to provide a framework for safe, lawful and secure sharing of information between members of the Board to protect vulnerable adults with care and support needs from abuse.

Sharing personal information is essential for delivering effective and efficient public services that meet the needs of people and safeguard the individual. The UK Information Commissioner (ICO) has written that a reluctance to share information in clearly appropriate circumstances "is one of the biggest challenges facing the public service today".

This document has been designed to encourage the safe, lawful and secure sharing of personal information between the police, health services, local authorities and their partners as part of the work of the Safeguarding Adult's Board.

This work has drawn heavily on the work of Gloucester Information Sharing Agreement.

Full acknowledgement and thanks is therefore given to our Gloucester colleagues.

Adoption of this Partnership Agreement as a basis for sharing and for developing Specific Information Sharing Agreements), where they are required, is essential for building the common approaches and improvement across services that are needed to ensure practice is safe, legal and secures public confidence. A Specific Information Sharing Agreement template has also been developed and incorporates in-built guidance to assist accurate completion.

Contents

1. Introduction & Purpose

1.1. Introduction

The purpose of this Partnership Agreement is to enable service-providing organisations directly concerned with the safeguarding, welfare and protection of the wider public to share relevant, minimum and appropriate personal information between them in a lawful, safe and informed way.

The Partnership Agreement can be adopted by all public sector organisations. In particular it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

Adoption of the Partnership Agreement will help ensure compliance with statutory and legislative requirements for disclosing personal data including the Data Protection Act 2018, the General Data Protection Regulation (GDPR), the Human Rights Act 1998 and with common law duty of confidentiality. It also enables compliance with the Information Commissioner's statutory Data Sharing Code of Practice.

Its implementation adds significant value to the delivery of effective and efficient public services that meet the needs of those receiving them.

The conditions, obligations and requirements set out in this agreement and supporting documentation will apply to all appropriate staff, agency workers, volunteers and others working on behalf of the partner organisations including agents and sub-contractors.

The Partnership Agreement will be reviewed after 3 years.

1.2. The Agreement for Sharing Personal Information.

The Partnership Agreement identifies the commitments required by each organisation to enable sharing of personal information. Sign up and ownership is at the highest level.

It is a statement of the principles and assurances which govern the activity of information sharing. It ensures that the rights of all those who are involved in the process are protected.

The Partnership Agreement will be supported within organisations by Specific Information Sharing Agreements.

Specific Information Sharing Agreements focus on the purposes underlying the sharing of specific sets of information between multiple organisations. They are intended for operational use and document the processes for sharing regular information, the specific purposes served, the people they impact upon, the relevant legislative powers, what data is to be shared, the consent processes involved, any required operational procedures and the process for review.

1.3. Information Excluded from the Information Sharing Partnership Agreement

Under the Information Sharing Partnership Agreement, there is no requirement to develop Specific Information Sharing Agreements to cover the exchange of information where it is considered to be either of an ad-hoc nature or on an infrequent basis. However, organisations must still consider the relevant compliance issues in line with the ICO's Data Sharing Code of Practice.

In addition there are two further broad categories of information relating to personal information that organisations may share without the need for protocols or agreements. These are:

Aggregated (Statistical) Information Aggregated and management information is used to plan and monitor progress of the organisation in its delivery of services. This is generally outside the scope of the Data Protection Act 2018 and the GDPR on the basis that a living individual could not be identified from such data.

Depersonalised and Anonymised Information that has had all personal information removed so as to render it anonymous and therefore outside the scope of the Data Protection Act 2018 and the GDPR.

Care must be taken with all aggregated, depersonalised and anonymised information to ensure that it is not possible to identify individuals e.g. in areas of low population density/low occurrence, as this would then still be classed as personal information.

2. Organisation Commitments

2.1. Introduction

This section outlines the principle commitments that each signatory organisation will make by adopting the Information Sharing Partnership Agreement. When fully implemented these should ensure that the organisation's treatment of personal information is compliant with current legislation and good practice.

2.2. Individual Users' Rights

Each organisation will comply with the rights of the individual in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance. Each organisation must ensure that they have appropriate policies and procedures in place to facilitate both the protection and the exercising of these and other rights.

Each organisation must be clear and open with individuals about how their information will be used. In general terms an individual should be told the identity of the organisation collecting and recording the data. The reasons or purpose for doing so (including any statistical or analytical purposes), and any extra information that an individual needs in the circumstances to ensure that their information is being processed fairly. This is known as a 'Privacy Notice' and complies with Principle 1 of the Data Protection Act 2018 and Principle A of the GDPR.

Each organisation must also inform individuals about their additional rights in respect of legislation and how these may be exercised. This will include the provision of appropriate support in order that individuals may best exercise those rights e.g. providing information in alternative formats or languages, providing support in the form of advocacy or assisting them to make a subject access request.

Individuals generally have the right under Article 18 of the GDPR to request the restriction of processing on the use and disclosure of certain personal information and need to be made aware of this right by participating organisations. It should not be assumed that individuals are content for their personal information to be used for purposes other than those directly associated with their receipt of services from the organisation to which they provided their information.

Individuals generally have the right under Article 16 of the GDPR to request the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the individual has the right to have incomplete personal data completed, including by means of providing a supplementary statement.
Individuals generally have the right under Article 17 of the GDPR to be forgotten. Unless certain grounds for processing apply.

Each organisation shall, under Article 19 of GDPR, communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 of the GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the individual about those recipients if the data subject requests it.

Individuals generally have the right under Article 20 of GDPR to receive the personal data concerning them, which they have provided to an organisation, in a structured, commonly used and machine-readable format and have the right to transmit those data to another organisation, where technically feasible, without hindrance.

Individuals generally have the right under Article 21 of GDPR the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions.
Individuals generally have the right under Article 22 not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

All individuals have the right to expect that information disclosed by them or by other parties about them to an organisation will be protected, managed and processed

with the appropriate degree of privacy and confidence. However, individual's rights to prevent disclosure of their personal information may be overridden in certain circumstances in accordance with legislation and common law.

2.3. Consent

All individuals must be informed as to the circumstances in which their consent will be required before their personal information may be shared. The details provided must include what personal information is recorded and why, what future use will be made of it and the length of time it is likely to be retained. The individual should also have explained to them the possible consequences of refusing or withdrawing consent and the exceptional circumstances in which a decision may be taken to share without consent.

Individuals will be informed that they are entitled to limit the disclosure of their information in accordance with their preferences, except where exceptional circumstances apply.

Individuals have the right to object to information they provide in confidence being disclosed to others in a form that identifies them, even where the latter are providing essential care or services.

Information may only be shared without consent in circumstances where it is justified and compatible with the requirements of current legislation, common law and any current guidance.

Specific Information Sharing Agreements should provide the conditions which must be met before information can be shared and the circumstances in which information can be shared without consent.

Reasons that lead to a decision to proceed with a disclosure without consent must be fully documented. Wherever practical and possible participating organisations must inform the individual of the decision and the reasons for it and indicate the legal basis on which the disclosure is permitted or required.

If an individual lacks capacity and is unable to consent to a specific disclosure/sharing of information, any decision to share personal information about them without consent can only be made if it is in their best interests.

The person reaching a decision as to the best interest of the individual will take into account the following:

- The individual has previously expressed or recorded wishes;
- Views of any legal guardian or a person holding valid Lasting Power of Attorney;
- Views of a carer or other person close to the individual, including paid carers;

Safeguarding Children Normally personal information about children will not be shared without the consent of the child themselves (if they are over the age of 12) or a person with parental responsibility. However, in situations where there is reasonable cause to suspect that a child or young person is suffering or is likely to

suffer significant harm, children's social care must carry out a section 47 investigation.

All agencies have a responsibility to inform children's social care and to share information if they are concerned that a child or young person is in need or at risk of harm. It is good practice to seek consent from the family before doing this, however if this could increase the risk to the child or young person, information should be shared without consent as safeguarding the child is paramount.

2.4. Staff and Others with Access to Information

Each organisation must have in place internal operational policies and procedures that will facilitate the effective processing of personal information which is relevant to the needs of the organisation, its managers, staff and users.

Staff contracts must contain appropriate confidentiality clauses that detail possible consequences of unauthorised or inappropriate disclosure of personal information.

Staff should be made aware of the Data Protection Act 2018 offences outlined in Appendix A.

2.5. Organisations are required to demonstrate they comply with the principles of GDPR under Article 5(2) which states explicitly that this is their responsibility.

Each organisation must ensure that all relevant staff receive training, advice and ongoing support in order to be made aware, and understand the implications of:

- This Information Sharing Partnership Agreement and Specific Information Sharing Agreements. This should include any associated procedural requirements arising from their implementation;
- The law which applies generally and in relation to the performance of the specific statutory powers and functions of the participating organisation concerned;
- Any Codes of Practice or other associated legislation, regulations and guidance.

Each organisation must have in place disciplinary procedures which could be invoked if a member of staff intentionally breached the confidentiality of a service user or intentionally shared information in a manner that is incompatible with the Data Protection Act 2018 and the GDPR.

Where a partner organisation relies on a third party to process personal information on their behalf, the organisation must have an appropriate contract in place.

2.6. Data Protection Act Notification

The Data Protection (Charges and Information) Regulations 2018 requires every organisation or sole trader that processes personal data to notify the ICO of their processing activities and pay the data protection fee, unless they are exempt. It is

the responsibility of each organisation to ensure that its entry is kept accurate and up to date, failure to do so is a criminal offence.

2.7. Subject Access Requests

Organisations must fully comply with all valid Subject Access Requests made under Article 15 of the GDPR.
If a request is received by an organisation which would also cover another organisation's information they should inform, and request the views of, the other organisation prior to release of the information. Each organisation should do this within the statutory timescales.

Each organisation must have in place policies and procedures that will facilitate the effective processing of Subject Access requests.

2.8. Freedom of Information

This Information Sharing Partnership Agreement should be disclosed under the Freedom of Information Act 2000 and should become part of your Publication Scheme.

Where partner organisations are not bound by this legislation consideration should still be given to referencing this information on their website.

2.9. Records Management

Inaccurate, incomplete or out of date information can have a detrimental effect on individuals. Therefore each organisation is responsible for the quality and accuracy of the personal information it holds.

If it is discovered that information held is inaccurate, partner organisations must ensure that their records/case management systems are corrected or updated accordingly. The organisation will take reasonable steps to advise any other party known to have received or to be holding that information about the change which it is necessary to make.

All participating organisations will have policies and procedures in place which will make clear their approach to retention, storage and disposal of records.

2.10. Information Security

Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and shared.

Each organisation must ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, information risk management, systems development, role based security access levels, secure receiving and transfer of data and system specific security policies.

Each organisation must consider the impact on individuals' privacy before developing any new IT system or changing the way they handle personal information. Please note that the ICO has published advice and guidance on Data Protection Impact Assessments, which is available on their website.

It is accepted that each organisation will vary in size and complexity and this will be reflected in their policies, processes, procedures, organisational structures and how they achieve effective information security.

2.11. Professional Ethics and Codes of Conduct

Partner organisations will recognise that individual professionals are accountable to their regulatory body for complying with their respective codes of conduct. Each organisation will take into account these requirements before reaching any decision to share information accordingly.

3. Information Sharing Partnership Agreement and Specific Information Sharing Agreement Process

3.1. Adoption of the Information Sharing Partnership Agreement

All organisations wishing to use a Specific Information Sharing Agreement for the sharing of information will need to be signed up to the Information Sharing Partnership Agreement. When signing up to the Information Sharing Partnership Agreement each organisation must identify a Designated Person who will have responsibility for implementing and monitoring the organisation's commitments. This will include supporting the adoption and dissemination of the Information Sharing Partnership Agreement within the organisation.

This Designated Person will usually be the person with overall responsibility for personal information within the organisation, such as the Senior Information Risk Owner (SIRO) or Caldicott Guardian.

The Designated Person may delegate day to day responsibility to individuals with operational responsibility for Information Governance and Data Protection.

Each Information Sharing Partnership Agreement Designated Person for the organisation agrees to support the adoption, dissemination, implementation, and review of this Information Sharing Partnership Agreement and its requirements in accordance with its own internal and any other jointly agreed and authorised information governance standard and/or operational policies and procedures.

The Designated Person must satisfy themselves that, in adopting the agreed standards and good practice, their organisation will work towards the principles and assurance set out in the Information Sharing Partnership Agreement

The 'Declaration of Acceptance and Participation' should be completed and signed by the Designated Person, to confirm adoption of the Information Sharing Partnership Agreement. A copy of this declaration is at the end of the Information Sharing Partnership Agreement

Once this has been completed a copy should be sent to the relevant Information Governance Team:

Information Governance
North Tyneside Council
Quadrant
The Silverlink North
Cobalt Business Park
North Tyneside
NE27 0BY

Information Governance
Northumberland County Council
A197
Morpeth
Northumberland
NE61 2EF

A record will be held of all signatories by the Information Governance Team.

3.2. Specific Information Sharing Agreement Process

Once an organisation has signed up to the Information Sharing Partnership Agreement Specific Information Sharing Agreements (SISAs) can be created.

SISAs should be completed by individuals with an operational knowledge of how the sharing will take place. All organisations included in the SISA should contribute to the creation of the document.

The signatory should be a senior member of staff such as a Caldicott Guardian, Director or equivalent.

The SISA should be completed and signed by both sharing organisations. A signed copy should be held by both organisations. A copy of the SISA template can be found at the end of the Information Sharing Partnership Agreement

Individual organisations are responsible for their own SISAs.

Each organisation is responsible for the audit, monitoring and publishing of its own SISAs.

3.3. Concerns and Complaints

Any concerns or complaints received relating to the processing/sharing of any personal information will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation. Any complaints relating to non-compliance may also be raised with other partner organisations if appropriate.

4. Glossary of terms

GDPR General Data Protection Regulation
SISA Specific Information Sharing Agreement
MOPI Management of Police Information

5. Document History

Date	Version	Change type	Details

Appendices

Appendix A

Data Protection Act 2018 and GDPR offences

The GDPR modernised offences to ensure that prosecutions continue to be effective and these have been transposed into UK domestic law by-way of the Data Protection Act 2018. The current offences are as follows:

Section 170 (1)(a) to knowingly or recklessly, without the consent of the Data Controller, obtain or disclose personal information;

Section 170 (1)(b) to knowingly or recklessly, without the consent of the Data Controller, procure the disclosure to another person;

Section 170(1)(c) to after obtaining personal data, to retain it without consent of the person who was the Data Controller in relation to the personal data when it was obtained

Section 170(4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).

Section 170 (5) A person who offers to sell personal data is guilty of an offence if

(a) he has obtained the data in contravention of subsection (1), or

(b) he subsequently obtains the data in contravention of that subsection.

Section 171(1) to knowingly or recklessly re-identify information that is de-identified personal data without the consent of the Data Controller responsible de-identifying the personal data
Section 171(5) to knowingly or recklessly to process personal data that is information that has been re-identified where the person does so-

(a) Without the consent of the Data Controller responsible for de-identifying the personal data, and

(b) In circumstances in which re-identification was an offence under subsection (1)

Section 173(3) creates an offence for the Data Controller, a person employed by the Data Controller, an officer of the Data Controller or subject to the direction of the Data Controller to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

Appendix B - Specific Information Sharing agreement

This information sharing agreement reflects the reasons, processes and procedures for sharing personal data.

North Tyneside and Northumberland Specific Information Sharing Agreement

Purpose

The organisations involved have signed up to the overarching principles set out in the Information Sharing Partnership Agreement and these principles must be adhered to. Once information is shared with another organisation they become the data controller of the shared copy of the information and are responsible and accountable for the use and protection of it.

This agreement:

- sets out the legislative basis for the legitimate sharing of personal information in specific circumstances between two or more data controllers.
- will be supplemented by relevant procedures and standards is to be completed by Information Asset Owners (or their delegate), project, process or service managers or an Information Governance Specialist.
- can only be signed by a Caldicott Guardian or Director (or equivalent).

This sharing agreement is not appropriate in circumstances where:

- one organisation engages another to undertake work on its behalf; in these cases information governance must be detailed within a contract; or
- one-off sharing is needed.

This agreement sits below the North Tyneside and Northumberland Information Sharing Partnership Agreement

1. Parties to the agreement:

Parties	**Name and address of organisation**
Party 1 North Tyneside Council Northumberland County Council	Quadrant, Silverlink North, Cobalt Business Park, North Tyneside NE27 0BY County Hall, A197, Morpeth. NE61 2EF.
Party 2 Northumbria Police	
Northumbria Healthcare Foundation Trust	
Northumbria Tyne and Wear Mental Health Trust	
Northumberland Fire and Rescue Service	

National Probation Service	
Community Rehabilitation Service	
North Tyneside Clinical Commissioning Group	
Northumberland Clinical Commissioning Group	
Tyne and Wear Fire and Rescue Service	

2. Why is this sharing required?

The Safeguarding Adult's Board is responsible for the implementation of policies and procedures that strategically and operationally address the way in which issues that cause harm to people with care and support needs are minimised. This includes understanding demand and performance, understanding what has happened in cases so that lessons can be learned, development and implementation of strategies and operational procedures, training and development for staff and working with provider agencies to improve service quality.

3. What information is to be shared?

x Personal Data

x Special Categories of Data (see definitions)

Please select all that apply and then describe the information below, e.g. name, date of birth, address, health details etc.

Description of the information to be shared:

Information will be Personal Data such as name address date of birth, NINO, and Special Category Data such as NHS number, relationships, health and social care history, education history, police and housing information. These are examples however the nature of the safeguarding role of the Board means that all information held by the parties to the agreement could be shared. This will include not only vulnerable adult's own information but could also include information pertaining to significant others connected to that person.

Much of the information will be able to be provided in anonymised or even statistical form but serious cases may be identifiable to members of the Board.

4. Frequency

How often will the sharing take place?

Boards are held quarterly but this agreement also applies to the sub groups of the Boards. Specific pieces of work will have their own timescales

If ad hoc or other, please detail the circumstances when sharing will be appropriate:

5. Legislative basis

Please select all that apply and provide the name of the relevant piece(s) of legislation below.

x Information **MUST** be shared by law

☐ Information **MAY** be shared by law

☐ Information **MAY** be shared, but only with CONSENT

Details of the relevant legislation:

Data Protection Act 2018
General Data Protection Regulation (EU) (2016/679)
Equality Act 2010
Local Government Act 1972
Localism Act 2011
Children Act 2004 Section 10 – general duty to improve well-being
Children Act 2004 Section 11 – duty to safeguard and promote the welfare of children
Care Act 2014

6. How the GDPR Principles will be met

Each Party will need to detail how the GDPR requirements below will be achieved. Links should be provided to relevant procedures. (Links to the organisations intranets will only be accessible to those with access). **Requirement Personal data are:**	**Party 1 -**	**Party 2-**
(a) processed lawfully, fairly and in a transparent manner in relation to individuals;	**Delete as appropriate:** ● Explicit written consent is received at the point of assessment ● Information will be shared without consent with relevant MASH partners only if the conditions re lawful condition for processing are met	**Delete as appropriate:** ● Explicit written consent is received. ● Individuals are given a leaflet at the time of collection. ● Individuals are informed over the telephone at the time of collection.

	• Individuals are given written information at the time of assessment. • Information is available online. Link to privacy notices on website: https://mycare.northtyneside.gov.uk/web/portal/pages/privacy https://www.northumberland.gov.uk/NorthumberlandCountyCouncil/media/About-the-Council/information governance/Northumberland-County-Council-Full-Privacy-Notice.pdf	• Information is available online. Link to privacy notices on website: • Posters are displayed in public areas, details: • n/a – not the organisation collecting the data • other:
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;	The point of contact for this agreement will ensure that the information is only used for the purposes that individuals are informed about, or as required by law. Information sharing decisions will be documented for audit, monitoring and investigation purposes	The point of contact for this agreement will ensure that the information is only used for the purposes that individuals are informed about, or as required by law. Information sharing decisions will be documented for audit, monitoring and investigation purposes
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	The point of contact for this agreement will review the data being shared quarterly to ensure that sufficient, but not too much, information is being shared.	The point of contact for this agreement will review the data being shared every to ensure that sufficient, but not too much, information is being shared.
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	The organisation will ensure that data is accurate through regular data cleansing exercises and regular case file audits, If the party notices any errors in the data they will notify the relevant point of contact within days of becoming aware.	Please describe how you ensure data is accurate e.g. Data quality strategy, regular data cleansing exercises, controls are in place for data entry, etc. Links: If the party notices any errors in the data they will notify the relevant point of contact within days of becoming aware

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;	The point of contact for this agreement will ensure that suitable entries are within their organisation's retention schedule and these are adhered to.	The point of contact for this agreement will ensure that suitable entries are within their organisation's retention schedule and these are adhered to. Link to retention schedule:
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	**The data will be shared by:** (delete/add as appropriate) Secure file transfer Secure email e.g. Egress, Cryptshare Secure access to system, AIS, CCM LiquidLogic arrangements, **Delete/add as appropriate:** The party meets the following information governance assurance standards : N3 PSN ISO27001 Specific procedures for the security of personal data are available on request. Approved disposal methods: Contract for secure shredding, LiquidLogic The point of contact for this agreement will ensure that suitable information security incident procedures are in place.	**The data will be shared by:** (delete/add as appropriate) Secure file transfer Secure email e.g. Egress Post, nhs.net, pnn.police.uk Encrypted removable media, e.g. memory stick Secure access to system, name of system As part of joint working arrangements, **Delete/add as appropriate:** The party meets the following information governance assurance standards : N3 PSN ISO27001 Specific procedures for the security of personal data are detailed at . Approved disposal methods: (link) **Add more links to specific guidance as required.** The point of contact for this agreement will ensure that suitable information security

		incident procedures are in place. Link:
Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."	**The organisation must:** ● Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies. ● Maintain relevant documentation on processing activities. ● Where appropriate, appoint a data protection officer. ● Implement measures that meet the principles of data protection by design and data protection by default. Measures could include: ● Data minimisation; ● Pseudonymisation; ● Transparency; ● Allowing individuals to monitor processing; and ● Creating and improving security	**The organisation must:** ● Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies. ● Maintain relevant documentation on processing activities. ● Where appropriate, appoint a data protection officer. ● Implement measures that meet the principles of data protection by design and data protection by default. Measures could include: ● Data minimisation; ● Pseudonymisation; ● Transparency;

	features on an ongoing basis. • Use data protection impact assessments where appropriate. You can also: • Adhere to approved codes of conduct and/or certification schemes. See the section on codes of conduct and certification for more detail.	• Allowing individuals to monitor processing; and • Creating and improving security features on an ongoing basis. • Use data protection impact assessments where appropriate. You can also: • Adhere to approved codes of conduct and/or certification schemes. See the section on codes of conduct and certification for more detail.
Transfers subject to appropriate safeguards You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.	Adequate safeguards may be provided for by: a legally binding agreement between public authorities or bodies; binding corporate rules (agreements governing transfers made between organisations within in a corporate group); standard data protection clauses in the form of template transfer clauses adopted by the Commission; standard data protection clauses in the form of template transfer clauses adopted by a supervisory	Adequate safeguards may be provided for by: a legally binding agreement between public authorities or bodies; binding corporate rules (agreements governing transfers made between organisations within in a corporate group); standard data protection clauses in the form of template transfer clauses adopted by the Commission; standard data protection clauses in the form of

	authority and approved by the Commission; compliance with an approved code of conduct approved by a supervisory authority; certification under an approved certification mechanism as provided for in the GDPR; contractual clauses agreed authorised by the competent supervisory authority; or provisions inserted in to administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.	template transfer clauses adopted by a supervisory authority and approved by the Commission; compliance with an approved code of conduct approved by a supervisory authority; certification under an approved certification mechanism as provided for in the GDPR; contractual clauses agreed authorised by the competent supervisory authority; or provisions inserted in to administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

(Add more columns for each party as required. You may also need to change the orientation of the document to landscape)

6. Review

This sharing agreement will be reviewed every 3 years or earlier if a significant change occurs such as further guidance and information produced on GDPR

If the Constabulary are party to this agreement to satisfy MOPI requirements it will be reviewed annually.

7. Supplementary documents

This agreement is to be supplemented by appropriate supporting documents, which may include:
Information Transfer Procedure, including detailed security arrangements
Information Risk Assessment

Data Protection Impact Assessment
Retention Schedule
Information Flow Map

8. Document information

Document owner:	Jacqui Old Director of Children's and Adult's Services (North Tyneside) Cath McEvoy-Carr – Director of Children's and Adult's Services (Northumberland)
Next review date:	June 2019
Version:	1.0
Summary of changes:	

9. Point of contact for each party

	Name	Role	Contact Details
Party 1 - This will be the person who completed the agreement. (This person will be the document owner. They will be responsible for adherence to, review, monitoring and advice in relation to the agreement.)	Ellie Anderson Steve Smith	Assistant Director Business Assurance – North Tyneside Data Protection Officer	Ellie.anderson@northtyneside.gov.uk 0191 6437354 steve.smith@northumberland.gov.uk
Party 2 –			

10. Signatories

	Name	Role (Please delete as appropriate)	Signature	Date
Party 1 -	Jacqui Old Cath McEvoy-Carr	**Director**		
Party 2 -		**Caldicott Guardian / Director /or equivalent**		

(Add more rows as required)

Appendix C – Definitions of personal and special category data

Personal data

Any information that identifies a living individual. This includes, but is not limited to, name, data of birth, NI number, medical diagnosis, address, employee number.

You may think information has been anonymised, but the legal definition takes into account other data held by the organisation. Therefore, if you hold the key to identify people from the anonymised data, then it is still covered by the Data Protection Act and the General Data Protection Regulation.

Special categories of personal data:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation
- Genetic data, biometric data processed for the purpose of uniquely identifying a natural person

Appendix D GDPR Conditions for Processing

6(1)(a) – Consent of the data subject
6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
6(1)(c) – Processing is necessary for compliance with a legal obligation
6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject
Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

Appendix E Conditions for special categories of data

If you are processing special category data you must be able to meet one of the conditions in Appendix E and one in Appendix F.

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
9(2)(e) – Processing relates to personal data manifestly made public by the data subject
9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Appendix F Declaration of Acceptance and Participation form

This signature is hereby given as confirmation that the following organisations are a signatory to the Information Sharing Agreement. I will be the signatory and representative for this organisation.			
Organisation	Signatory Name and Role	Signature	Date
North Tyneside Council			
Northumberland Council			
Northumbria Police			
Northumbria Healthcare Foundation Trust			
Northumbria Tyne and Wear Mental Health Trust			
Northumberland Fire and Rescue Service			
National Probation Service			
Community Rehabilitation Service			
North Tyneside Clinical Commissioning Group			
Northumberland Clinical Commissioning Group			
Tyne and Wear Fire and Rescue Service			
