On completion of this agreement and BEFORE signing the contract, Legal Services MUST be consulted before ANY data is shared.

Northumberland County Council

Data Sharing Agreement

Northumberland County Council and Channel Panel Partners

Version: 1.0
Unique IG Reference (*supplied by IG*): DSA/21/003

Version control:

Version	Date	Amended by	Description	Review Date

Contents

Date of agreement: 23/02/22

1. MULTI-AGENCY INFORMATION SHARING

1.1 The aim of this agreement is to define how personal data and special category (Sensitive) data processed by Northumberland County Council and Channel Partners will be shared and why. This document is a binding agreement between these organisations and outlines what measures must be taken by partners to this agreement to comply with relevant Legislation concerning personal and special category data.

2. DEFINITIONS

2.1 In this agreement "**Personal Data**" means any data which relate to an individual who can be identified directly or indirectly by an identifier such as (but not limited to);

a) Name
b) Date of birth
c) Address
d) GP

2.2 In this agreement "**Special Category Data**" means confidential personal data consisting of information that relates to an individual, as to;

a. their racial or ethnic origin,

b. their political opinions,
c. their religious beliefs or other beliefs of a similar nature,
d. whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e. their physical or mental health or condition,
f. their sexual life or sexual orientation,
g. genetic or biometric data

"**Shared Personal Data**" means the personal data [and special category data] to be shared between the parties, described in Appendix A of this Agreement.

"**Data Controller**" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

"**Data Protection Legislation**" means all applicable data protection in force from time to time in the UK including (but not limited to) the UK General Data Protection Regulation ('GDPR') and the Data Protection Act 2018 relating to personal data, and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data.

"**Data Subject**" means an individual who is the subject of personal data.

"**Third Party**" means any person other than;

a. the data subject,
b. the data controller, or
c. any data processor or other person authorised to process data for the data controller or processor.

"**Data Protection Authority**" means the relevant authority set up to uphold information rights in the public interest (Information Commissioner's Office).

"**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

"**Data Processor**" means any person who processes the data on behalf of the data controller.

"**Processing Data**" means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

a. organisation, adaptation or alteration of the information or data,
b. retrieval, consultation or use of the information or data,
c. disclosure of the information or data by transmission, dissemination or otherwise making available, or
d. alignment, combination, blocking, erasure or destruction of the information or data.

3. PARTIES

3.1 This Data Sharing Agreement applies to the following listed organisations:

Organisations:
Northumberland County Council
Northumbria Police
Northumbria Healthcare NHS Foundation Trust
Northumberland Clinical Commissioning Group
Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust
Northumberland Fire and Rescue
Northumberland college
Northumberland Probation Service

together: 'the Parties'

4. PERIOD

4.1 The agreement shall commence on the date stated at the beginning of it.

4.2 This agreement will be reviewed annually to ensure that it fulfils its intended purpose and that no changes are required. The review will take place between the parties to the agreement. Should changes be needed in advance of the annual review, these should be discussed with the parties who will decide what action to take.

5. POWER

5.1 This agreement is written with the following relevant legislation/ Code of Practices applied:

a. The Data Protection Act 2018
b. UK GDPR
c. Counter-Terrorism and Security Act 2015 (CTSA)
d. Human Rights Act 1998
e. Health and Social Care Act 2008
f. The Care Act 2014
g. Confidentiality Code of Practice
h. Records Management Code of Practice

6. PURPOSE

6.1 This agreement sets out the framework for sharing of personal data and special category data between the parties as Data Controllers. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

6.2 The parties consider this data sharing initiative necessary in order to support the national Prevent strategy and comply with statutory

functions set out in Section 36 of the Counter Terrorism and Security Act.

6.3 The aim of this agreement is to facilitate the work of the Channel Panel which forms a key part of the national Prevent strategy. Channel is multi-agency process, providing support to individuals who are at risk of being drawn into terrorism (the “Agreed Purpose”). Sharing information is in support of the statutory function set out in Section 36 of the Counter Terrorism and Security Act.

6.4 The data sharing will serve to benefit individuals and society by enabling local organisations becoming more effective and efficient in their delivery of health and social care and in the prevention in counter terrorism and security threats.

7. COMPLIANCE WITH GDPR AND THE DATA PROTECTION ACT 2018

7.1 Any personal data, including special category data, held by the parties and managed by it or on its behalf by a third party, is held on the proviso that the data has been processed in accordance with the Data Protection Legislation.

7.2 Each party must ensure compliance with the Data Protection Legislation at all times during the term of this agreement.

7.3 The legal basis for the sharing of personal data by Channel panel representatives has been identified as:

Article 6(1)(e) GDPR: the 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. Clause 8 of the Data Protection Act provides that Article 6(1)(e) includes (a) processing of personal data that is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and (b) processing of personal data that

is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department. Processing of personal data for Channel is necessary for the purposes of the various Channel duties set out in section 36 of the Counter-Terrorism and Security Act 2015 (CTSA).

7.4 In addition to its obligations under clause 7.3, the legal basis for the sharing of special category data by Channel panel representatives has been identified as:

Article 9(2)(g) GDPR and paragraph 6 of Part 2, Schedule 1 DPA 2018 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 parties for the discharge of a statutory function as set out in section 36 of the CTSA 2015.

7.5 All parties to this data sharing agreement, in respect of shared personal data, shall review and ensure that their privacy notices are clear and provide sufficient information to the concerned data subjects for them to understand what personal data is being sharing, the circumstances in which it will be shared, the purposes for the data sharing and either the identity of the parties or a description of the type of organisation that will receive the personal data.

8. PROCESS

8.1 The table below sets out the process for which the Channel Panels follows to ensure it meets its obligations under the data protection legislation.

Source of the information i.e., staff/ services/ systems	• The source of the information is a multi-agency collaboration where information is

	shared. • The agencies include those outlined in 3.1.
How information will be shared between partners	• Only information which is needed by the panel in the discharge of their duties is shared via a monthly meeting with Chair and core members of each agency. This information should be vetted before being shared. • Documents are shared via a secure SharePoint that only core members can access. • Emails are shared but do not contain personal information. • Monthly updates are uploaded to the SharePoint alongside the minutes.
Frequency of information being shared	• Information is shared on a monthly basis in the meetings and updates are uploaded monthly to the SharePoint.
How information will be checked for accuracy	• The Chair is requested to sign off all minutes and updates to the SharePoint before the next meeting.
Where will information be stored and how data stored will be secure by each partner to the agreement	• The information is stored on a SharePoint site that only core members of each agency have access to. • Some sections of the SharePoint are restricted further and can only be access by the Chair. • All members of the channel panel must sign a confidentiality statement which is renewed annually. • The Chair confirms at the start of each monthly meeting that all confidentiality statements have been signed and are up to date. This is recorded within the minutes of

	the meeting. • There is also a clear notice on front page of SharePoint about the confidentiality obligations of those involved.

8.2 This Data Sharing Agreement is made for the purposes of sharing data between Channel Partners as described in clause 6.2 (the **Agreed** Purpose). Shared personal data is any data to be processed under the provision of the section 36 of the Counter-Terrorism and Security Act 2015 described in Appendix A and described in this clause.

8.3 The parties agree to only process shared personal data, as described in Appendix A. The parties shall not process shared personal data in a way that is incompatible with the purposes described in this clause (the **Agreed** Purpose).

8.4 Each party shall appoint a single point of contact (SPoC) who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative. The SPoC for each of the parties are outlined in Appendix B.

8.5 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the shared personal and special category personal data in accordance with Authority policy and procedures, together with any other applicable provisions of the Data Protection Legislation and associated guidance.

8.6 Having considered the relevant provisions of the Data Protection Legislation and associated guidance, the Parties should have in place their own process that must be followed in the event of a Data Breach.

8.7 The Parties shall ensure that all Channel Panel members will sign the confidentiality declaration as outlined in clause 13.

8.8 The Parties agree to ensure that any breach relating to the data, including but not limited to any suspected or actual loss or compromise of the data, must be handled and reported as soon as possible and no later than within 72 hours in line with local policy and the GDPR/ Data Protection Act 2018.

8.9 All respective partners to this agreement have a duty to inform all relevant signatories to this agreement if a subsequent data breach is on their part and may also impact them as a result of a breach concerning information shared under this agreement.

9. RETENTION

9.1 Information will be retained in line with the relevant organisation's retention schedules.

9.2 Staff should review individual cases files on a case by case basis, taking into account any outstanding subject access requests.

9.3 All signatories to this agreement accept responsibility for ensuring that all appropriate security arrangements are complied with. Any issues concerning compliance with security measures will form part of the annual review of this agreement.

9.4 Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures of the individual partner agency.

9.5 All parties are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

9.6 All partners will hold a copy of this agreement. It is the responsibility of each partner to ensure that all individuals likely to come in contact with the data shared under this agreement are trained in the terms of this agreement and their own responsibilities.

10. INFORMATION RIGHTS REQUESTS

10.1 Data Subjects have the right to obtain certain information about the processing of their personal data through Subject Access Request including circumstances where the processing of a Data Subject's personal data is not in compliance with the Data Protection Legislation. Data Subjects may also request rectification, erasure or restricted processing of their personal data.

10.2 SPoCs are responsible for maintaining a record of individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The points of contact for each party are detailed in Appendix B.

10.3 The parties agree to provide reasonable assistance as is necessary to each other to enable them to comply with Subject Access Requests and to respond to any other queries or complaints from data subjects.

11. PROHIBITIONS

11.1 No personal data or special category data must be disclosed to any third party without the written consent of the parties to this agreement.

11.2 Personal data or special category data will not be extracted from the party's systems onto any mobile device, laptop or other electronic device, other than those provided by the respective parties of the Channel Panel agreement.

11.3 Personal data or special category data may only be accessed remotely by the parties via secure connections and only in an environment that affords a level of suitable security and privacy.

11.4 Any provision in this agreement does not prejudice the right or obligation of any party to share the personal or special category information where required by law or an order of a court.

12. PRECAUTIONS

12.1 All partners to this Data Sharing Agreement each shall ensure:

a. implementation of appropriate technological and security measures against unauthorised or unlawful processing of the data are implemented, to safeguard against accidental loss, destruction or damage to the data, included ensuring that all equipment/devices are up to date (patched);
b. there is secure physical storage and management of any non-electronic data;
c. That access to the data is restricted to personnel that require it, taking reasonable steps to ensure the reliability of employees who have access to the data, such as ensuring that all staff have appropriate background checks;
d. That they will comply with the confidentiality provisions as set out in clause 13.

12.4 Data shared through this agreement must be managed securely and not disclosed to another third party, except for the purpose specified within the 'Process' section of this agreement. Failure to abide by this principle may constitute a breach of the Data Protection Act 2018.

13. CONFIDENTIALITY

13.1 Each party shall ensure that all information discussed is strictly confidential and must be treated as such during or subsequent to any Channel Panel meeting. Information shared should be directly or indirectly relevant to cases on a need-to-know basis. Any subsequent handling of any information considered at this meeting and must not be disclosed to third parties without the prior agreement of the parties to this agreement.

13.2 All parties will ensure that the minutes of each Channel Panel meeting are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to race, gender, sexuality and disability.

13.3 The responsibility to take appropriate actions rests with each party. The role of the Channel Panel is to facilitate, monitor and evaluate effective information sharing to enable appropriate actions to be taken to increase public safety.

13.4 Each party will ensure that all Channel Panel members will sign the confidentiality declaration at the start of each meeting.

14. PENALTIES

14.1 The Data Discloser and Data Receiver undertake to indemnify each other and hold each other blameless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this agreement.

14.2 In the event of a dispute or claim brought by a Data Subject or the Information Commissioner Office concerning the processing of shared

personal data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

14.3 The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Information Commissioner Office. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

15. SIGNATORIES

Organisation	Northumberland County Council
Name	[redacted]
Position	Executive Director of Adult Social Care & Children's Services and Deputy Chief Executive
Phone Number	[redacted]
Email	[redacted]@northumberland.gov.uk
Date	21st March 2022
Signature	[redacted]

Organisation	Northumbria Healthcare NHS Foundation Trust
Name	[redacted]
Position	Executive Medical Director & Caldicott Guardian
Phone Number	[redacted]
Email	[redacted]@northumbria.nhs.uk
Date	28.2.22
Signature	[redacted]

Organisation	Northumbria Police
Name	[redacted]
Position	Counter Terrorism Case Officer
Phone Number	[redacted]
Email	[redacted]@NORTHUMBRIA.POLICE.UK
Date	16/5/2022
Signature	[redacted]

Organisation	Northumberland Clinical Commissioning Group
Name	Siobhan Brown
Position	Chief Operating Officer
Phone Number	01670 704850
Email	Siobhan.brown3@nhs.net
Date	8/4/2022
Signature	[redacted]

Organisation	Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust
Name	[redacted]
Position	CNTW PREVENT lead
Phone Number	[redacted]
Email	[redacted]@cntw.nhs.uk
Date	04.03.2022
Signature	[redacted]

Organisation	Northumberland College (City of Sunderland College)
Name	[redacted]
Position	Head of Corporate Governance & Policy
Phone Number	[redacted]
Email	[redacted]@educationpartnershipne.ac.uk
Date	18.05.2022
Signature	[redacted]

Organisation	Northumberland Fire and Rescue
Name	[redacted]
Position	Prevention Manager
Phone Number	
Email	[redacted]@northumberland.gov.uk
Date	16 May 2022
Signature	[redacted]

Organisation	Northumberland Probation Service
Name	
Position	
Phone Number	
Email	
Date	
Signature	

Appendix A – Data to be Shared

Classification	Data Item	Data Discloser	Data Receiver
Personal Data	Any data shared within the statutory provisions of the GDPR and DPA 2018. For example: Name Address		

	Postcode Gender Date of Birth Living Arrangements Family and personal relationships Statutory Education Neighbourhood Lifestyle		
Special Category Data	Any data shared within the statutory provisions of the GDPR and DPA 2018. For example: Ethnicity Criminal proceedings / Offending history Religious Belief Political Affiliation Sexual Life/ Sexual Orientation Cultural Factors Thinking and behaviour Emotional and Mental Health Attitudes to engagement in relevant activity Motivation for Change Substance Misuse Risk posed to self and others Motivation to change Perceptions of self		

Appendix B – Single point of contact (SPoC)

Organisation	Northumberland County Council
Name	[redacted]
Position	Prevent Lead
Phone Number	[redacted]
Email	[redacted]@northumberland.gov.uk
Date	16/05/2022

Organisation	Northumbria Healthcare NHS Foundation Trust
Name	[redacted]
Position	Head of Safeguarding
Phone Number	[redacted]
Email	[redacted]@nhct.nhs.uk
Date	16/05/2022

Organisation	Northumbria Police
Name	[redacted]
Position	Counter Terrorism Case Officer
Phone Number	
Email	
Date	

Organisation	Northumberland Clinical Commissioning Group
Name	
Position	
Phone Number	
Email	
Date	

Organisation	Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust
Name	[redacted]
Position	
Phone Number	
Email	
Date	

Organisation	Northumberland Fire and Rescue

Name	
Position	
Phone Number	
Email	
Date	

Organisation	Northumberland College
Name	
Position	
Phone Number	
Email	
Date	

Organisation	Northumberland Probation Service
Name	
Position	
Phone Number	
Email	
Date	