

[Insert Additional Organisational Logo(s)]

[Title of agreement]

Information Sharing Agreement

Based on the Derbyshire Partnership Forum Information Sharing Protocol v 5.1



All Information Sharing Agreements must be sent to [the organisation] Information Governance or Legal Department for initial review and registration.

Document Status

|  |  |
| --- | --- |
| Version | [insert…Latest version number of the ISA] |
| Document owner | [insert…Organisation name] |
| Document author and enquiry point | [insert…Name]  [Job Title]  [Contact Details] |
| Document authoriser | [insert… Name and Job Title of whomever has approved this ISA i.e. Director, Head of Service, DPO, Caldicott Guardian etc.] |
| Document agreed date | [insert…date all parties have agreed and signed up to the ISA] |
| Document classification | [insert…Public / Controlled / Restricted] |
| Document distribution | [insert…list partners organisations] |
| Document retention period | [insert…for example: 3 years from document review/end date] |
| Next document review/end date | [insert… date appropriate for this ISA which may depend on your data, 1 or 2 years or change to data and or data processors and sub processors in which case a whole document review may be required and possibly a revised Privacy Impact Assessment] |

Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Date Issued | Version | Status | Reason for change |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

See Derbyshire Partnership Forum Information Sharing Protocol version 5.0 for guidance on completion. <http://www.derbyshirepartnership.gov.uk/about_us/>

## Introduction

Insert a brief introduction, examples below. Set out any Term and abbreviations here also

* 1. This Information Sharing Agreement (Agreement) has been developed to facilitate partnership working between the partners identified in 2.1 below (Parties}. This Agreement identifies the legal powers and methods of sharing information in order to achieve common goals for the benefit of the Derbyshire Area.
  2. This Agreement outlines the need for [insert] to work together to [insert] etc.
  3. All Parties to this Agreement should ensure that all of their staff who are affected by it are aware of its contents and the obligations it creates between the Parties signed up to it.

## Partner and partner responsibilities

### The Parties committed to this Agreement are:

Who are the intended Partners to this Agreement and what are their responsibilities? Including Data Controller, Data Processor and Sub Data Processors (third parties)

* + - [name of organisation] who has the role of Data Controller
    - [name of organisation(s)] who has the role of Data Processor(s)
    - [name of organisation(s)] who has the role of Data Sub-processor(s) - remove if not applicable

### It will be the responsibility of these Parties to ensure that they:

* + - have realistic expectations from the outset
    - maintain ethical standards
    - have a process by which the flow of information can be controlled
    - provide appropriate training
    - have adequate arrangements to test compliance with the agreement
    - meet Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR) and other relevant legislative requirements.

## Background and scope of the Agreement

What is the purpose of the agreement? What is the specific business need/objective for information sharing? What are the benefits to sharing these data? Has a Privacy Impact Assessment (PIA) been carried out on this business process? If not, start with your organisations PIA screening questions.

* 1. It has been identified that in order to…
  2. The Agreement covers the sharing of personal data about data subjects for the purpose of [Enter here] and the Agreement covers sharing for any of the purposes listed in Section 5: ‘Purposes and legal basis for Sharing Information’.

## Information to be shared

What specific information is required for the purpose of this agreement? List fields of Information to be shared, do these cover special categories of data, personal data? Give consideration to the identifiability of individuals. (See section 4 of the Protocol for more information on types of data). Could list in a table…

### Data to be shared

4.1.1. It has been identified by the Parties that the following fields of data are required to fulfil the purpose and scope of the Agreement as identified in 3.1 and 3.2.

4.1.2. These data are to be provided by [enter Party one here] and are to be received by [enter other Party / All remaining Parties]. If any third party processing via a sub processor, detail it here also.

### Data Processing

Detail any processing of the data to be carried out by any of the Parties. In particular, document processing of any special categories of personal data.

### Terms of use of the information

Add a clear statement of how the information is intended to be used and any restrictions which may apply. Consider the enhanced rights of the individual, take Consent and the Right to be forgotten into consideration. Is there a Privacy Notice in place for these data? If so, does this Agreement fit with the agreed terms of re-use (if any)? Could also specify named individuals who would be the responsible for processing the data etc.

### Exchange of Information

State explicitly how and what information is to be shared, consider methods such as encrypted email, mail, secure file transfers and how regularly these are to take place.

## Purposes and legal basis for information sharing

### Purpose for sharing information

The main purpose for sharing information is to… how will services be improved, what value does the data have, what value will be added by any data processing activity?

### Legal Basis for Sharing Information

5.2.1. The legal basis for sharing information between the Parties has been identified as …State Legal basis for information sharing. What are the specific lawful powers/obligations for the processing of information?

What considerations apply to make the processing fair under the terms of the Data Protection Act 2018 or GDPR? (see Appendix 4 and 5 of the Derbyshire Partnership Information Sharing Protocol (https://www.derbyshirepartnership.gov.uk/site-elements/documents/pdf/information-sharing-protocol.pdf) or for full DPA 2018 visit [http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga\_20180012\_en.pdf](http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf%20).

### Other legislation which has an impact on the Agreement

Could include a brief description of the main impact of relevant legalisation and can have an appendix to list all relevant legislation (if applicable), see [Appendix 3](https://www.derbyshirepartnership.gov.uk/site-elements/documents/pdf/information-sharing-protocol.pdf) of the Derbyshire Partnership Information Sharing Protocol for examples of other legalisation that could be considered.

## Data Quality

Explain what standards will apply for data quality and how errors will be handled. Taking the GDPR principles and rights for individuals into consideration as well as principles 3 and 4 of the DPA 2018 (see Appendix 4 and 5 of the [Derbyshire Partnership Information Sharing Protocol](https://www.derbyshirepartnership.gov.uk/site-elements/documents/pdf/information-sharing-protocol.pdf)), for example:

* 1. Information shared under this Agreement must be fit for purpose, meaning that it must be adequate, relevant and not contain excessive detail which is beyond that required for the agreed purpose.
  2. Where information received by any partner is insufficient to achieve the agreed purpose, i.e. inaccurate, out-of-date or inadequate for the stated purpose clarification will be sought with the Data Controller before the information is acted upon. Partner’s receiving such queries will act promptly to resolve them, ensuring corrections are documented and cascaded to all Parties without delay.

Appropriate records will be kept to record sources of information and any methodologies applied when processing the data.

## Retention, Storage and Disposal

Explain how long the information is intended to be retained for the purpose, how the data will be stored and any specific security, review or disposal arrangements that apply.

### State explicitly how long the data is to be held for by all Parties if the Data Controller intends for the Data Processors to only keep these data for a specified period in accordance with the Data Controllers retention policy, otherwise could say in line you’re your organisations retention policies.

7.2 All Parties must ensure that they have appropriate measures in place to ensure the secure storage of all the information subject to this Agreement will be kept as follows:

* + - Physical copies of information provided should be held in a lockable storage area, office or cabinet
    - Electronic files must be protected against illicit internal use or intrusion by external parties through the appropriate security measures

7.3 How are the Parties expected to dispose of the data at the end of the retention period?

## Access and Security

Explain the standards and conditions which are required to protect the information concerned. Include any special arrangements which might apply. For example access to files will be restricted – operate a clear desk policy, employees given access on a need to know basis. Is there any specific training needed or is a basic or enhanced Disclosure and Barring Service (DBS) check required?

## Handling of complaints, information requests or breaches of the Agreement

### Handling of data breaches

9.1.1. Data processors, will in the event of a personal data breach or breach of confidentiality take steps to notify the Data Controller and relevant organisations Data Protection Officer(s) (DPO) as soon as possible. The Data Controller has the responsibility to notify the ICO of a serious breach within 72 hours of any signatory organisations becoming aware of the breach. See section 9 of the Protocol for more information.

Detail the relevant DPO contact information. Organisation will be required to record all information about any personal data breaches.

### Indemnity to the Agreement

9.2.1. Each Party will keep each of the other Parties fully indemnified against any and all costs, expenses and claims that arise out of any breach of this Agreement by their staff, agent, contractors or data processors and in particular, but without limitation, the unauthorised or unlawful loss, theft, use, destruction or disclosure by the offending Parties or its sub-contractors, data processors, employees, agents or any other person within the control of the offending Parties of any data obtained in connection with this Agreement.

### Handling of complaints

9.3.1 Any Party, on receipt of a complaint, without delay must…

### Handling of requests for information under Data Protection / FOI

9.4.1 Where the [non Data Controller], in response for [insert] information made under the Freedom of Information Act 2000, or the Environmental Information Regulations 2004 or a Subject Access Request, as applicable is considering disclosing [insert] information obtained via this Agreement it will consult with [Data Controller] before doing so.

9.4.2 The [non Data Controller] will, in fulfilling obligations under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004, or Subject Access Request, as applicable, comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) where the [insert] information includes personal and/or special category data.

## Commencement and Termination of the Agreement

### Commencement of the Agreement

10.1.1 This Agreement shall take effect from the date that the Parties fix their signatures below and shall continue in force for as long as the pilot phase continues or until this Agreement is terminated under Section 10.2 below.

### Termination of the Agreement

10.2.1 Any Party may terminate this Agreement at any time provided they give a minimum of 30 days’ notice in writing to the other Parties.

10.2.2 Any Party can suspend this Agreement for 30 days if they consider that security arrangements have been compromised. Such suspension arrangements are intended to allow the affected Party the opportunity to seek a resolution and cause any remedial actions to be completed. In the event that agreement is not reached, the Agreement will be terminated in writing with full explanation to the Parties concerned.

10.2.3 The obligations of confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

## Monitoring, review and dissemination of the Agreement

Detail the procedures and process for monitoring the implementation of the ISA. Specify the review period for the ISA and name the individual who will be responsible for the review process (normally the document author).

### Monitoring of the Agreement

Detail the procedures and process for monitoring the application of the ISA and detail the responsibilities for monitoring of all Parties. Will the procedures, methods and data be reviewed by the Data Controller during the life of the Agreement? i.e the Audit team review the measures, training, security etc. If the process, methodology or data quality are not what the Data Controller expects…

### Review of the Agreement

11.2.1 All Parties agree to review the Agreement every two years or when there is any major change to the data, process, relevant legislation or Parties to the Agreement. The Parties agree to notify a representative of the Data Controller of any requirements to review the Agreement and it will be the responsibility of the Data Controller to instigate the review.

### Dissemination of the Agreement

* + 1. All Parties will disseminate copies of this Agreement to all relevant staff and, on request, to the data subjects of the Agreement process and will ensure that appropriate training is provided to all relevant staff.

## Signatories

Ensure all organisations have agreed to and signed the Agreement **before** information sharing takes place. Check your organisations approval procedures as it may require your Data Projection Officer (DPO), Caldicott Guardian, Senior Information Risk Officer (SIRO), Information Governance lead officer or Director to agree and sign this Agreement.

**Data Controller:** Insert Organisation name

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Name & Title/Role |  | Signature |  | Date |

**Data Processor:** Insert Organisation name

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Name & Title/Role |  | Signature |  | Date |

**Data Processor:** Insert Organisation name

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| Name & Title/Role |  | Signature |  | Date |