1. Partners/signatories

You should list each organisation which will be sharing information under this ISA and someone from each of these organisations will be a signatory.

2. Purpose - Why do you need to share this information?

You should explain why sharing this information will help each of the signatories.

We need to share this information because XXXXXXXXXXX.

Specifically information is shared to achieve:

- ......
- ......
- ......

3. Legal Basis – What law allows you to share this information?

Information must be shared lawfully. If you are a public authority you can only work within legal framework which relates to your organisation. (Ultra vires rule) The Data Protection Act 1998 does not give a legal basis to share information it provides guidelines which help you share information fairly and lawfully.

Link to Key public sector responsibilities and their legislative basis to these can be dropped in to the ISA.

You need to remember that some information is protected from sharing or disclosure by legislation or Home Office guidance (certain health information, convictions) so you need to make sure that no such restrictions apply to the information you want to share.

If you are sharing personal information you need to identify which Schedule 2 condition(s) of the Data Protection Act applies. Hyperlink to Schedule 2 conditions. Cut and paste from the hyperlink the relevant conditions.

These are the Schedule 2 conditions which apply: -

If you are sharing sensitive personal information Hyperlink to definition of sensitive personal data you need to identify which Schedule 3 condition(s) of the Data Protection Act (1998) apply. Hyperlink to Schedule 3 conditions – include Order 417 2000. Cut and paste from the hyperlink the relevant conditions.
These are the Schedule 3 conditions which apply:

These are how all 8 Principles of the Act are met.  

Hyperlink to compliance with the 8 DP Principles

4  Do we need to consider the Human Rights Act 1998?

If you are sharing information which relates to a person’s private and family life, their home or their correspondence they have a right to respect under Article 8 of the Human Rights Act 1998. This means you can only share this information when it is lawful and necessary to achieve one or more of these aims. Hyperlink to Article 8, Cut and paste from the hyperlink the relevant conditions.

These are aims which apply to satisfy Article 8:

Necessary means that you only share the minimum amount of information - you should only share information when it is necessary to do so not because it would be nice to know. Consider how you would feel if this was your information which was being shared.

5  What Information does each signatory need to share? And what will this information be used for? Will anyone else have access to this information?

The easiest way to show this is probably to complete the table below

You also need to agree who is the Data Controller.

In most circumstances when you give information to another organisation they will take ownership of that information which means that it is their Chief Executive/Officer who is the Data Controller (Hyperlink to definition) and becomes legally responsible for making sure that the information is held and used in compliance with the Data Protection Act 1998.

If some of the signatories are organisations which your organisation has contracted or agreed will provide a service on your behalf (these may be other public sector organisations, voluntary organisations, charities, etc) you should contact your Information Management section for guidance about who is the Data Controller. You will need to make sure that there is a contract or agreement in place which makes clear their responsibilities for using your organisation’s information.

If the way in which you are sharing information involves the use of a shared computer application where the signatories can all add,
amend or delete information there may be Joint Data Controllers or Data Controllers in Common. Joint Data Controllers covers the situation where the determination is exercised by acting together equally. “Determination in common” is where data controllers share a pool of personal data, each processing independently of the other’.

In this case you will need to include an indemnity at Section 4 of this ISA.

<table>
<thead>
<tr>
<th>Providing Organisation</th>
<th>Receiving Organisation</th>
<th>Who is the Data Controller</th>
<th>Information to be shared</th>
<th>What will this be used for</th>
<th>Who will have access to this information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hyperlink to example

No data will be forwarded on to a third party or sub-contractor without the express written permission of the original data controller.

6  **Indemnity**

Do you need an indemnity Yes/No. If Yes, then copy the indemnity from the hyperlink.

Hyperlink to wording of indemnity

7  **How are you going to keep information accurate?**

Explain how you are going to do this

8  **How long will the information be kept?**

Each organisation which has received information referred to in this agreement is likely to have their own policy which says how long they will keep different types of information – this should be on their web sites. You can either create a hyperlink to each of these policies or you can simply state for each organisation how long they will keep the information. Sometimes this may be a number of years but in other cases an organisation may keep information as long as they are working with the individual and then for a certain number of years afterwards in order to comply with a legal requirement.

E.g.

X Organisation will keep the shared information for ………………. /or a period of …… years.
Y Organisation will keep the shared information for ……………… /or a period of ….. years.

9  How will we share and keep information secure?

Hyperlink to security table. Fill in the sections of the table that are required and attach that to this ISA as Appendix A

Hyperlink to PIA template

10  What if we want to use the information for something else?

If any organisation wishes to use the information which they have been given under this agreement for any purpose other than that in Section 2 above, they must first ask the organisation which provided the information for their written consent.

11  What do we do if information is lost, disclosed, misused, etc?

If any information which is shared under this agreement is lost, stolen, or disclosed to someone who should not have seen it this is not only a breach of confidentiality but is likely to be a breach of the Data Protection Act (for which the Data Controller can be fined up to £500,000). If the information is deliberately accessed and/or disclosed by someone who is not entitled to see or use it this person may have committed a criminal offence under the Data Protection Act 1998 or the Computer Misuse Act 1990. Information may be deleted when it should have been kept. These are all information breaches.

It is important that the organisation(s) which provided the information are told as soon as possible so that they can risk assess what has happened – they may need to tell individuals what has happened to their information and they may need to tell the Information Commissioner. An investigation may have to be done by the police or the Information Commissioner so evidence (audit trails, printouts, etc) may need to be recovered.

The organisation where the breach occurred may need to do an internal investigation and this may lead to disciplinary action or identify processes which need to be changed.

Each organisation should provide contact details of the post in their organisation who should be informed if an information breach occurs in the table below.

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Post</th>
<th>Email</th>
<th>Telephone</th>
</tr>
</thead>
</table>

12  How will you check if your colleagues are complying with this agreement and if it is still current?
Each organisation should agree how and when they are going to check if the information they receive is being used in accordance with this Agreement. This should be included here.

You should all review this agreement after one year from signature so enter the date …………………. After this it should be reviewed every five years unless there has been some change (legislation, need to extend organisations involved, etc) which needs the agreement to be updated.

13 What happens if there is a major security breach?

Any organisation can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and provide evidence of what went wrong. A representative from each organisation should meet asap (no longer than 14 days) to carry out a Risk Assessment and Resolution meeting.

Termination of this ISA should be in writing to all other Partner Organisations giving at least 30 days’ notice.

14 What do we do if we are asked to disclose information which we receive under this ISA?

You may receive a request under the Freedom of Information Act 2000 or the Data Protection Act 1998. In Leicester, Leicestershire and Rutland it has been agreed that when an organisation receives a request for information which has been shared under an ISA the organisation which receives the request will tell the organisation which provided the information and ask for their views about the disclosure of the information so this can inform the decision making process.

15 Who are the Responsible People in each organisation?

Information sharing activity should be reviewed and approved by the organisation's legal/information security staff.

Each organisation should give details of the post which is responsible on a day to day basis for monitoring compliance with this ISA.

On behalf of xxx organisation:

Post or Name: Xxxxxx
Address: xxxxxxx
Tel: xxxxxxx
Email: xxxxxxx

On behalf of xxx organisation:

Name: Xxxxxx
Address: xxxxxxx
16 **Who are the Appropriate Signatories in each organisation?**

*Each Partner should identify who is the most appropriate post holder within their agency to sign the ISA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their organisation to the agreement. Don’t forget this is the person who is making the commitment on behalf of the organisation that the conditions in this ISA will be complied with.*

Signed on behalf of **xxxx organisation**:

Name  __________________________
Role  __________________________
Signature  __________________________
Organisation  __________________________
Date  __________________________

Signed on behalf of **xxxx organisation**:

Name  __________________________
Role  __________________________
Signature  __________________________
Organisation  __________________________
Date  __________________________
<table>
<thead>
<tr>
<th>Sharing &amp; Destruction Methods</th>
<th>Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation Data Network (e.g. internal email)</td>
<td>Recommend passwording attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title, or sensitive personal data in body of email. Use of GCSx network where available. Recommend turning off autofill of address field.</td>
</tr>
<tr>
<td>Email between partners</td>
<td>Passwording attachments for sensitive personal data in case it is sent to wrong email address. No personal data in subject title, or sensitive personal data in body of email. To/from Police: Restricted or sensitive personal data only to emails using PNN, GSI, CJSM or MOD secure addressing conventions or via GCSx and PSN connections. To/From NHS: Secure transfer as agreed with health partners (currently under discussion county-wide due to new health arrangements - To be updated when agreed).</td>
</tr>
<tr>
<td>Laptops, removable media, USB, etc</td>
<td>Must be owned by the employer and encrypted. No personal information from any of the organisations in this ISA is to be loaded to personally owned removable media.</td>
</tr>
<tr>
<td>Electronic storage of information</td>
<td>Has the application where it will be stored been pen tested? In other words, could someone hack into it? Check with your IT department. How will access to the information be restricted. Please say how this will be done. Is there an audit trail which will show</td>
</tr>
<tr>
<td>Topic</td>
<td>Instructions</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Vetting/clearance of staff</td>
<td>Have the staff who will receive and access the information been vetted.</td>
</tr>
<tr>
<td>Internal and public telephone network</td>
<td>May be used.</td>
</tr>
</tbody>
</table>
| Mobile telephone (voice and text)                          | Digital cell phones may be used.  
Only use analogue cell phones if operationally urgent, use guarded speech and keep conversation brief. |
| Fax                                                        | Note faxes are legacy technology and are NOT to be used unless there is no alternative. If no alternative, check recipient is on hand to receive.  
Send cover sheet first and wait for confirmation before sending. |
| Storage of papers                                          | Protected by one barrier, e.g. a locked container within a secure building/room. Locked filing cabinet for storage if home working. |
| Disposal of papers                                         | Use secure waste sacks if organisation has system in place and make sure they are secure when left unattended or collected for destruction.  
Shred personal information if it is very sensitive. |
| Disposal of magnetic media                                 | All types of discs and other storage devices – dismantle and destroy by disintegrating, pulverising, melting or shredding then dispose with normal waste/recycling following destruction. |
| Movement within organisation via internal mail             | In a sealed envelope with protective marking shown. |
| Movement between partner agencies                          | By post or courier in a sealed envelope. |
| Movement between workplace and home / mobile office        | On encrypted memory stick or lockable briefcase. Locked filing cabinet for storage if home working. |
* If organisations do not find it possible to apply the appropriate security this should be discussed with the originator.