**PURPOSE SPECIFIC INFORMATION SHARING AGREEMENT (PSISA)**



The Agreement

TITLE:

**Document History**

This document has been distributed to:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Released to | Comments/Changes made |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Links to other Information Community Agreements or Purpose Specific Information Sharing Agreement (PSISA)s:**

|  |  |  |  |
| --- | --- | --- | --- |
| Agreement Title | Date & Version | Lead Agency | Contact details |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Template**

Please refer to the accompanying guidance notes when completing this form.

|  |  |
| --- | --- |
| **1 What** **category of data under the Data Protection Act is being shared?** | **YES/NO** |
| Data to be shared is classified as Personal Data |  |
| Data to be shared is classified as Sensitive personal Data |  |
| Data to be shared will be anonymised |  |
| Data to be shared will be psuedonymised |  |

|  |
| --- |
| **2 Who will I be sharing information about?** |
|  |

|  |  |
| --- | --- |
| **5 3 For what purpose is the information being shared?** | |
|  | |
| Is the information being shared for Primary Purposes | YES/NO |
|  |  |
| Is the information being shared for secondary purposes | YES/NO |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **4 What information will be shared?** | | | |
| 1. **Description of data/information:** | 1. **Field:** | 1. **Extracted from which system/Derived from:** | 1. **Agency Name:** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 1. **Frequency of data sharing** | One off: Y/N | Routine: Y/N |
| 1. **Other relevant information:** | | |

|  |  |  |
| --- | --- | --- |
| **5 Who might I be sharing with?** | | |
| **Agency & Lead Contact details:** | **Provider** | **Recipient** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| **6 Can I legally share this information?** | |
| **(A)Legislation** | **(B) Duties** |
|  |  |
|  |  |
|  |  |
| **(C) Data Protection Act 1998** | Under **Schedule 2** of the DPA, either of the following conditions can be met:  Under **Schedule 3**, the following conditions can be met:  It is also important to ensure that other Data Protection principles are complied with, for example the information being shared is relevant to the purposes of this agreement and is not excessive; information being shared is accurate and up to date; information is kept for no longer than necessary; information shared is kept secure. |

|  |  |
| --- | --- |
| **7 Do I need to obtain consent?** | |
| (A) Are you relying an on implied statutory power to share? | Y/N |
|  | |
| (B) Are you relying on consent? | Y/N |
|  | |

|  |  |
| --- | --- |
| **8 What am I telling Service Users about this information sharing & how are they notified?** | |
| (A) Is the information being shared for a different purpose other than that set out in each agency’s fair processing notice on how we use information? | **Yes** – go to A1  **No** – go to B |
| (A1) Provide the link to each Agency’s privacy notice | |
| (B) How will individuals be notified of the data sharing under this agreement? | |

|  |  |  |  |
| --- | --- | --- | --- |
| **9 How and when might I share information?** | | | |
| (A) Role/ person sending/receiving data | (B) Organisation | (c) Method of Secure Transfer | (D) Frequency of Transfer |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10 How will shared information be recorded and held?** | | | |
| (A) Organisation | (B) Location/Technical arrangements | (C) Duration | (D)Destruction |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **11 Who else can access this information?** |
|  |

|  |  |
| --- | --- |
| **12 Handling Breaches** | |
| (A) Name and contact details of person who is to be informed of breach | |
| Agency | Name and contact details |
|  |  |
|  |  |
|  |  |
| (B) Timescales |  |

|  |
| --- |
| **13 Other measures or considerations** |
|  |
|  |
|  |

|  |  |
| --- | --- |
| **14 Review of this agreement** | |
| Name/Role of Reviewers: |  |
| Date of Initial Review |  |
| Date of Consequent Reviews: |  |

Annex 1

**Purpose Specific Information Sharing Agreement (PSISA)**

In respect of

***(Insert Title)***

**DECLARATION OF ACCEPTANCE & PARTICIPATION**

Signed by, for and on behalf of: Page 1 of

|  |  |
| --- | --- |
| Organisation |  |
| Name |  |
| Position |  |
| Contact Details:  Phone:  Email: |  |
| Signature: |  |
| Date: |  |

|  |  |
| --- | --- |
| Name of agency contact for sharing information under this Purpose Specific Information Sharing Agreement (PSISA) |  |
| Position |  |
| Contact Details:  Phone:  Email: |  |
| DPA Registration Number & Date of Renewal: |  |

*Each agency who signs up to this agreement is to complete this form. Please print off as required.*

Annex 2

**Purpose Specific Information Sharing Agreement (PSISA)**

*(Insert Purpose Specific Information Sharing Agreement (PSISA) Title)*

**Master List of Signatory Organisations & their Designated Person’s**

Page 1 of

|  |  |  |  |
| --- | --- | --- | --- |
| Agency | Designated Person & Position | Contact Details  (telephone & Email Address) | Date when agency signed up to this PSISA |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Please insert, complete and print additional sheets as required.

**Purpose Specific Information Sharing Agreement (PSISA) – Guidance Notes**

**General**

See Wolverhampton Overarching Information Sharing Protocol – **Section 4 - Structure** for an overall description of the Information Sharing three tier approach and the different elements.

In order to share appropriate information between partners there must be a lawful, defined and justifiable purpose(s) which supports the effective delivery of a policy or service that respects people’s expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. This in turn must be supported by robust business processes.

The questions in this document are designed to ‘walk’ Managers/Practitioners/Designated Person’s and other specialist support (e.g. Legal, Technical, Data Protection, etc) through a process that should help fulfil this objective.

**Scope**

* This Purpose Specific Information Sharing Agreement (PSISA) is the third element of the information sharing framework. It is aimed at an organisations “operational management/practitioner” level and it will define the relevant business processes which support information sharing between two or more agencies for a specified purpose.
* Those Managers/Practitioners/Designated Persons negotiating this Purpose Specific Information Sharing Agreement (PSISA) will have to complete Sections 2 to 14 inclusive.
* This Purpose Specific Information Sharing Agreement (PSISA) is supplementary to Wolverhampton Overarching Information Protocol (Tier 1), which must be consulted when drawing up this agreement, along with any Information Community Agreements that are in place and relevant to this Purpose Specific Information Sharing Agreement (PSISA).
* Partner organisations may belong to a variety of differing Purpose Specific Information Sharing Agreement (PSISA)s and Information Community Agreements.

Partners may use the information disclosed to them under a Purpose Specific Information Sharing Agreement (PSISA) only for the specified purpose(s) set out in that Purpose Specific Information Sharing Agreement (PSISA) document. They may not regard shared information as intelligence for the general use of their organisation unless they have defined and agreed this purpose within the Purpose Specific Information Sharing Agreement (PSISA) and have informed their respective service users of this use.

* Wherever this Purpose Specific Information Sharing Agreement (PSISA) impacts, or has a dependency, on another Purpose Specific Information Sharing Agreement (PSISA) then details of these must be entered into the Table at Section 2 of this document.

**Parties to this Purpose Specific Information Sharing Agreement (PSISA)**

* The parties to the Purpose Specific Information Sharing Agreement (PSISA) are those that have signed the Declaration of Acceptance and Participation (DAP) at the end of this document (See this Document Annex 1). This list, along with the details of each organisation’s ‘Designated Person(s)’ as shown on the ‘DAP’ and at Annex 2, will be updated and reissued on a regular basis.
* Any party to this Purpose Specific Information Sharing Agreement (PSISA) who is not already a party to Overarching Protocol, agrees to comply with the terms of the Overarching Protocol insofar as it is relevant to the information sharing under this Purpose Specific Information Sharing Agreement (PSISA).
* By signing this document all of the parties agree to accept and implement this Purpose Specific Information Sharing Agreement (PSISA) and to adopt the statements and procedures contained within it.
* Any purported breaches of, or other complaints about, this agreement will be dealt with in accordance with the processes described at [**Appendix E - Handling Breaches**](#_APPENDIX_E_-) of the Overarching Protocol.

**User Guide**

**1 What category of data under the Data Protection Act is being shared?**

Please select the category of data being shared.

* Personal Data – information that would identify a living individual such as name, date of birth, address etc.
* Sensitive Personal Data – personal data which consists of the following information:
  + The racial or ethnic origin of an individual
  + Political opinions
  + Religious beliefs or beliefs of a similar nature
  + Membership of a trade union
  + Physical or mental condition of an individual
  + Sexual life of an individual
  + The commission or alleged commission of an offence or
  + Any proceedings for any other offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.
* Anonymised Data – data which has had identifiers removed so that an individual cannot be identified.
* Pseudonymised Data – data which has had identifiers removed and replaced with a pseudonym.

The data being shared under this agreement is likely to be either personal or personal sensitive data, unless the information to be passed is entirely anonymised or statistical. Where if it is anonymised or statistical, you should give careful consideration to the possibility that an individual could nevertheless be identified from it – e.g. if it provides statistics on the ethnicity of crime victims in a limited geographical area it might inadvertently identify someone from an uncommon ethnic group in that locale. Pseudonymised information may be a consideration in these circumstances.

**2 Who will I be sharing information about?**

Please detail the types of service users whose information is being shared.

**3 For what purpose is the information being shared?**

Provide detail on the specific purpose for which personal information will be shared and the benefit that is to be achieved by sharing the information.

Please indicate whether the information sharing is for PRIMARY or SECONDARY PURPOSES.

**Primary Purposes** – this is information that is being shared for direct healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

**Secondary Purposes** – this is information being shared for non-direct healthcare and medical purposes - such as service improvement, performance management, reporting or commissioning.

**4 What information will be shared?**

1. List the items of information to be disclosed - for example Name, DOB, Address, Postcode,
2. List the data field name/criteria each item will be derived from.
3. List the system(s) from which each data field/record is extracted from/derived from
4. List the Agency from where the information is being sent from.
5. Detail the frequency of when the information is being sent. Is the information being shared as a one-off data sharing initiative - if so detail when the information is being sent. Is the information being shared on a routine basis – if so detail the frequency. If on the other hand you propose an agreement to make a series of individual disclosures in response to specific requests – sharing offender details at case conferences for instance -it may be necessary to be more general.
6. Are there any data quality issues, such as the accuracy, validity, timeliness and relevance of the data, if there are, then these should be considered here.

**5 Who might I be sharing with?**

Identify the relevant agencies/ organisations/practitioners and whether they are a provider or recipient of personal information or both.

**6 Can I legally share this information?**

Does your organisation have the vires (power) to share? Which particular legislative function is the data sharing taking place?

1. List the legislation/statutory duty that the information can be shared under.
2. List the relevant section and statutory duties that enable the sharing to take place.
3. Under the Data Protection Act 1998, what conditions in schedule 2 and/or schedule 3 of the Act can be met? If personal data is being shared then only 1 condition from schedule 2 needs to be met. Where sensitive personal information is being shared – then 1 condition from both schedule 2 and 3 need to be met.

|  |  |
| --- | --- |
| **Conditions for processing personal data under the DPA 1998.** | |
| ***Schedule 2 - Personal Data*** | ***Schedule 3- sensitive personal data*** |
| The individual who the personal data is about has consented to the processing. | The individual whom the sensitive personal data is about has given explicit consent to the processing. |
| For the performance of a contract to which the ‘individual’ is a party, or the individual has asked for something to be done so they can enter into a contract | The processing is necessary so that you can comply with employment law. |
| The processing is necessary because of a legal obligation that applies to the agency (except an obligation imposed by contract) | The processing is necessary to protect the vital interests of:  - the individual (in a case where the individual’s consent cannot be given or reasonably obtained), or  - another person (in a case where the individual’s consent has been unreasonably withheld). |
| The processing is necessary in order to protect the vital interests of the data subject. This applies in cases of life or death, such as where an individual’s medical history is disclosed to A&E treating the data subject following a serious road accident. | The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition. |
| The processing is necessary for exercising statutory, governmental, or other public function | The individual has deliberately made the information public |
| The processing is in accordance with “legitimate interests” condition | The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights. |
|  | The processing is necessary for administering justice, or for exercising statutory or governmental functions. |
|  | The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality |
|  | The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals. |

*See Appendix B and C of the Wolverhampton Overarching Information Sharing Protocol for further guidance.*

**7 Do I need to obtain consent?**

1. Are you relying on an expressed or implied statutory power to sharing? Refer to section 6 - is there a statutory power or legal duty that enables you to share information without consent? What conditions for processing are being met for the data you are sharing?
2. Are you normally going to rely on consent? If so describe how consent will be obtained, recorded and how long it will be valid for.

If consent is normally required to share information for this purpose; provide detail on any specific circumstances where this consent is not required.

Advice on consent is available from Appendix D in the Wolverhampton Overarching information sharing protocol

**8 What am I telling Service Users about this information sharing & how are they being notified?**

1. Identify whether the sharing of information under this agreement is covered by each relevant agency’s “fair processing notice”/Privacy Notice (See Appendix D – 13.1.6 and 13.1.7 of the Wolverhampton Overarching Information Sharing Protocol).
2. If the sharing of data is not covered under this agreement complete section B and describe how you are informing individuals of the data sharing under this agreement.

Also outline how and when this notification is provided to individuals. If applicable, outline the circumstances where the Service User will not be told about the information sharing. If the consent is due to last for a lengthy period of time, detail at what points/how often an individual will be reminded of the fair processing information and given a subsequent chance to “opt out” having previously given consent.

**9 How and when might I share information?**

1. Detail the role/name of persons sending or receiving data
2. Detail the name of the organisation sending or receiving the information
3. Detail the method of transfer – e.g. secure email, Secure FTP etc.
4. Detail the frequency of the transfer

**10 How will shared information be recorded and held?**

1. Name of organisation
2. How/Where will the information be stored by the receiving partner? Describe the physical and technical security arrangements each agency has in place?
3. Detail how long the information is being kept for. Do any operational retention periods apply? Can it be securely deleted once processed or do you need to keep if for a certain period of time after the transfer? The nature of the information to be shared will have a bearing on how long it should be held. Refer to your organisations record retention schedule for further guidance or discuss with the organisation(s) that is going to be providing the information.
4. Personal information must be securely disposed of in line with the requirement under the 7th Data Protection Principle. Describe how each agency will ensure that the personal data is securely removed from their systems and any printed copies securely destroyed at the end of the work for which it was intended, or on termination of the contract. For example - In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. Any hard copy will be destroyed by cross-cut shredding and secure re-cycling of the resulting paper waste.

**11 Who else can access this information?**

Access should be limited to a need to know basis, specify if any internal or external parties have access to the information. For internal staff specify any vetting arrangements in place.

**12 Handling Breaches**

1. Detail the specific point of contact details for reporting any data breaches or near misses under this agreement. Where possible detail a 2nd point of contact for Business Continuity purposes.
2. Detail the agreed timeframes that data breaches are to be reported. As soon as possible or no longer than 24 hours after the incident was identified.

Refer to Appendix E – Handling Breaches of the Wolverhampton Overarching Information Sharing Agreement for further information around handling breaches.

**13 Other measures or considerations**

Add in any other measures and considerations that you may need to document within this agreement. **Example text could be**:

* Information provided by the partner will be held securely, will not be transferred to a third party, and will be used only by appropriate staff for the purposes identified.
* Electronic copies of information will only ever be held on encrypted devices or servers, will not be e-mailed outside the receiving organisation, and if transferred onto portable devices (which must be encrypted), will be disposed of securely and permanently.
* The partner organisation will not keep the personal data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the services under this agreement. Where this is necessary, the partner organisation will keep an audit trail of which laptops/drives/devices the personal data are held on.
* Paper copies of information, and printouts of electronic information, will be held securely, transferred either by safe haven fax or couriered in sealed containers and shredded upon disposal.
* Personal identifiable data will only be provided where there is a need to have that level of detail, and it is within the scope of consent on use of information given by the individual.
* The partner organisation shall employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to comply with either the NHS Information Governance Toolkit to level 2, or the requirements of ISO/IEC 27001:2005 (ISO/IEC 17799:2005) as appropriate to the services being provided.
* The partner organisation shall ensure that only such of its employees who may be required by it to assist it in meeting its obligations under the Agreement shall have access to the Personal Data.
* The partner organisation shall ensure that all employees used by it to provide the services as defined in the Agreement have undergone training in the law of data protection, their duty of confidentiality under contract, and in the care and handling of Personal Data;
* The partner organisation agrees to assist the Data Owner promptly with all subject information requests which may be received from the data subjects of the Personal Data;
* The partner organisation shall not use the Personal Data for any purposes other than those formally agreed with the Data Owner.
* The partner organisation shall not disclose the Personal Data to a third party in any circumstances other than at the specific written approval of the Data Owner.
* The partner organisation is NOT permitted to sub-contract any of the processing, nor transfer the personal data to any third party, without explicit written agreement from the Data Owner.
* The partner organisation will NOT transfer the Personal Data to any other country without explicit written agreement from the Data Owner.
* The partner organisation will ensure that the personal data is securely removed from their systems and any printed copies securely destroyed at the end of the work for which it was intended, or on termination of the contract. In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets HM Government standards. Any hard copy will be destroyed by cross-cut shredding and secure re-cycling of the resulting paper waste.
* The partner organisation will indemnify the Data Owner against any costs, expense, including legal expenses, damages, loss, liabilities, demands, claims, actions or proceedings which the Data owner may incur as a result of any breach of this Agreement by the partner organisation.
* This protocol is an integral part of any data sharing Agreement between the signatories to the protocol and shall be governed by and interpreted in accordance with the laws of the United Kingdom.

**14 Review of this agreement**

When will this agreement be reviewed to assess its validity in future? (it is recommended that each agreement is review every 12 months). Who will undertake the review?

Insert text here