Information Sharing Agreement Template

**Information Sharing Agreement Template**

|  |  |
| --- | --- |
| **Document owner:** |  |
| **Commencement date:** |  |
| **Review date:** |  |
| **Classification:** |  |

1. **Partners to the agreement**

The Partners committed to this agreement are:

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

* Maintain ethical standards
* Meet Data Protection Act 2018 (DPA), General Data Protection Regulation (UKGDPR) and other relevant legislative requirements.
* Have a process by which the flow of information can be controlled
* Have adequate arrangements to ensure compliance with the agreement, including the provision of appropriate training

1. **Purpose** - **Why is this information being shared?**[Please explain why this data is needed and what benefits sharing this information will bring]
2. **Legal basis** – **What is the legal basis which allows the sharing of this information?**

[Please see accompanying Guidance for more detail and for additional wording which can be used in this section, for example when sharing special categories of data]

You may share data relating to children’s health and care as long as you can demonstrate a compelling reason to do so in law. All health and care providers are subjected to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to the common law duty of confidence and should be done in accordance with the Data Protection Act 2018, and UK GDPR.

The Data Protection Act 2018 imposes a number of obligations on organisations that process personal data. For processing to be lawful, conditions set out in certain schedules within the Act must be met. All processing of personal data must satisfy at least one condition in Schedule 2 whilst processing of sensitive personal data must also satisfy a condition in Schedule 3.

Consent is an option in both of these schedules but other lawful bases for sharing data exist which may be more relevant for children and young people’s care. Consent is not required if a different condition can be satisfied, e.g.:

**Schedule 2:**

* ***The processing is necessary for the exercise of functions of a public nature exercised in the public interest by any person.***

**Schedule 3:**

* ***The processing is necessary for medical purposes and is undertaken by—***

1. ***a health professional, or***
2. ***a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.***

As confirmed by the Information Commissioner and Information Governance Review, ‘medical purposes’ includes the purposes of preventative medicine, medical diagnosis and the provision of care and applies to care provided by social care organisations.

Under UK GDPR, to lawfully share personal data, you must identify an Article 6 condition. The most relevant Article 6 conditions for lawful processing that are available to all publicly funded health and/or statutory health and social organisations in the delivery of their functions are:

**6(1)(c) *Processing is necessary for compliance with a legal obligation to which the controller is subject***

or

**6(1)(e*) Public task: the processing is necessary for you to perform a task in the public interest or in your official functions, and the task or function has a clear basis in law.***

Special category data can only be processed or shared if you can also meet one of the conditions in Article 9 of the UK GDPR. Explicit consent is a condition under Article 9(2)(a) but the most relevant Article 9 conditions is likely:

**9(2)(h) Health or social care - *Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment of the management of health and social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.***

1. **What will the data be used for?**
2. **Controllers**

The parties to this agreement are identified as follows:

All Parties agree to assist the Controllers in ensuring compliance with their obligations as set out in the Data Protection legislation.

Each Controller shall deal with any individual rights request or complaint/query received from a Data Subject in relation to data originating from and held by them and in line with their legislative obligations.

All Parties shall notify a Controllers’ Data Protection Officer without undue delay (and in any event within twenty-four (24) hours of becoming aware) of an actual Personal Data Breach.

Any Party shall notify the other Parties if, in their opinion, any of the Controller’s instructions infringes the Data Protection Legislation.

1. **What information is to be shared?**
2. **How will accuracy of information be maintained?**

It is the responsibility of each party to ensure as far as possible the information they supply is accurate. Care should be taken when checking the accuracy of the information to be shared and the details of the person or organisation the information will be shared with.

All parties will ensure compliance with their internal data quality policy and procedures and should inform any relevant parties where data is found to be inaccurate and/or out-of-date. The relevant Controller will be responsible for correcting the data and informing relevant parties to maintain data integrity. Data will be reviewed in accordance with partner data quality policies and procedures, and in line with the review process within the SEND Code of Practice.

1. **How will information be kept secure?**[Please see accompanying Guidance for more detail and suggested wording on how to ensure information remains secure when shared and processed]

Information will be transferred via a secure web portal or industry standard secure email. In instances where information needs to be shared via alternative means, an appropriate secure method of transfer will need to be agreed beforehand by partner organisations (this could include encrypted files with industry standard security or confirmed delivery post).

Partners will store the data in a secure environment and control and limit access to it, in accordance with their Data Security Policies and in compliance with relevant data protection legislation.

The recipient organisation will ensure sufficient training and sanctions are in place for the failure to comply with the agreement or breaches by individual staff.

1. **Who will have access to the information?**

Access to the information shared under this agreement will only be granted to individuals identified within the partner organisations as having a legitimate need to process the information for the agreed purposes.

The information may only be shared with the partners named in this agreement. No data will be shared with any other third party, sub-contractor or any other Authority without the express written permission of the controller/s.

1. **How will data be disposed of?**

At the end of the retention period stated above, parties will make sure that all data, regardless of format, is destroyed in accordance with their own local policies and procedures and provide evidence that this has been carried out.

Alternatively, the data must be returned to the Controller/Controllers in an agreed format and removed from their system infrastructure to ensure compliance with Data Protection Legislation.

**12. Further obligations on all parties to the agreement to ensure security of the information shared**

The information is shared solely for the purposes identified within this agreement and shall not be processed for any other purpose without full review of the accompanying DPIA; this and any other agreement related to the sharing; fully informed permission obtained in writing from all parties to this agreement and in particular the Controllers of the data shared.

Each party will make sure they take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. In particular, each partner must make sure they have procedures in place to do everything reasonable to make accidental compromise or damage unlikely; deter deliberate compromise or opportunist attack; dispose of or destroy the data in a way that makes reconstruction unlikely; and promote discretion to avoid unauthorised access.

Each party will notify the other parties to this Agreement of any complaint received from any person about the sharing of data under this agreement or any correspondence from the Information Commissioner or other regulator regarding the sharing of data under this Agreement.

Each Party will notify the other Parties of the name, email address, and direct dial telephone number of any Data Protection Officer and promptly notify the other Parties of any changes to those details.

**10. How long will the information be kept?**

Each Party shall delete or return the data shared and processed under this Agreement (and any copies of it) on termination of the Agreement unless any Party is required by Law to retain the data or is otherwise directed by the Controllers.

1. **Monitoring and review of the agreement**

This agreement will be reviewed on [DD/MM/YYYY] and then every [\_\_\_\_] years.

The agreement may also be reviewed when there is any major change to the data, processes, relevant legislation or Parties in the agreement.

1. **Termination**

This Agreement shall commence on the date set out at the beginning of this agreement. Unless terminated in accordance with this clause, this Agreement shall terminate on [DD/MM/YYYY].

Any Party may leave this Agreement by giving [\_\_\_] Business Days’ notice in writing to the other Parties.

Without affecting any other right or remedy available to it, each Party may immediately terminate this Agreement by notice in writing to the other Parties if any other Party commits a material breach of any provision of this Agreement or any other Party repeatedly breaches any of the provisions of this Agreement.

1. **Dispute Resolution**

In the event of a dispute arising under this Agreement, authorised representatives of the Parties will meet to try to resolve the dispute within five Business Days of being requested in writing by any Party to do so. If the dispute remains unresolved, it will then be referred to a senior manager from each of the Parties who will use all reasonable endeavours to resolve the dispute within a further ten Business Days.

If the Parties are unable to settle the dispute by negotiation, they must, within 5 Business Days after the end of the ten Business Day period referred to above submit the dispute to an independent body or organisation agreed between the Parties. If the Parties are unable to agree on an independent body or organisation within that period then the dispute shall be submitted to the Centre for Effective Dispute Resolution (CEDR). The mediations will follow the mediation process of the independent body or organisation agreed by the parties or CEDR as appropriate.

1. **Responsible people in each organisation**

**[Partner 1]**

|  |  |  |  |
| --- | --- | --- | --- |
| [Name] | [Role] | [Email] | [Telephone number] |

**[Partner 2]**

|  |  |  |  |
| --- | --- | --- | --- |
| [Name] | [Role] | [Email] | [Telephone number] |

**[Partner 3]**

|  |  |  |  |
| --- | --- | --- | --- |
| [Name] | [Role] | [Email] | [Telephone number] |

1. **Notices**

Any notice given to a Party under or in connection with this Agreement shall be in writing in the English language and shall be sent by email to the relevant addresses set out below. Any notice validly given in accordance with the foregoing clause shall be deemed to have been received the following Business Day.

1. **Variation**

Any proposed changes to this Agreement, including the addition or removal of parties, the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be Processed must be notified promptly to the Information Compliance/Governance leads so that the impact of the proposed changes can be assessed. No variation of this Agreement shall be effective unless it is in writing and signed by all Parties to this Agreement.

1. **Signatories in each organisation**

**On behalf of [Partner 1]**

|  |  |  |  |
| --- | --- | --- | --- |
| [Name] | [Role] | [Email] | [Telephone number] |
| [Signature] | | | [Date] |

**On behalf of [Partner 2]**

|  |  |  |  |
| --- | --- | --- | --- |
| [Name] | [Role] | [Email] | [Telephone number] |
| [Signature] | | | [Date] |

**On behalf of [Partner 3]**

|  |  |  |  |
| --- | --- | --- | --- |
| [Name] | [Role] | [Email] | [Telephone number] |
| [Signature] | | | [Date] |