MAISP Tier 2 - Agreement for data sharing for social care related activity undertaken within Surrey

INTRODUCTION

This over-arching data sharing agreement covers a range of activities undertaken within Surrey which require organisations to share personal data relating to individuals for social care related purposes. This Agreement forms a Tier 2 Data Sharing Agreement under the Surrey Multi Agency Information Sharing Protocol (MAISP).

The Agreement is supported by Tier 3 Data Protection Protocols which provide supplementary information for specific activities being undertaken and confirm the exact organisations involved.

Version 1.1

Date agreement comes into force 25/11/2022

Date for review 25/11/2024

Organisation Name Surrey County Council

1. PURPOSE AND SCOPE

PURPOSE

The purpose of this agreement is to:

- Provide a framework for the sharing of personal data relating to individuals as part of a multi-agency approach for the purposes of the provision of social care and for social care related activities
- Ensure all partners involved in multi-agency working understand their responsibilities regarding information sharing
- Facilitate the sharing of relevant personal or sensitive information between partner organisations with respect and confidentiality, while safeguarding individuals' legal rights
- Promote trust between partner organisations and the public

SCOPE

This over-arching data sharing agreement covers a range of activities undertaken within Surrey which require organisations to share confidential personal data relating to individuals for social care purposes. The agreement forms a Tier 2 data sharing agreement under the Surrey Multi Agency Information Sharing Protocol (MAISP).

Organisations covered by this agreement

This agreement is for organisations within Surrey who provide support or promote social care which includes, but is not limited to:

- Charities and Voluntary Sector organisations
- Education Settings
- Local Authorities (district/borough council, unitary and/or county council)
- Police
- Probation Service
- Providers of services to the above

2. DATA PROCESSING AND IMPACT ASSESMENTS (DPIA)

A single DPIA has not been carried out that covers all of the processing under this agreement. Individual DPIAs have been carried out for various processing and data sharing under this agreement, and there are Tier 3 protocols for specific activities. These DPIAs detail the safeguards to be implemented to ensure that the sharing of data is fair and lawful.

3. LEGAL BASIS

Each signatory agency to this Protocol undertakes to co-operate fully with each-other within the parameters of the following legislative instruments:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Common Law Duty of Confidentiality

Legal basis for processing

Each signatory agency shall ensure that it processes shared personal data fairly and lawfully and on the basis of one of the following six legal grounds:

Consent	Vital interests
Contract	Public task
Legal Obligation	Legitimate interests

For multi-agency working for the purposes of social care, the lawful bases which are likely to be the most relevant are public task and legal obligation, as organisations have statutory duties which require co-operation and information sharing.

For special category data, the lawful bases which are likely to be most relevant are:

Article 9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law'

Article 9(2)(g) Substantial public interest and Schedule 1, Part 2 (18): Safeguarding of children and of individuals at risk

Article 9(2)h "processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services"

Relevant legislation includes, but is not limited to:

Care Act 2014 - This puts in place a framework for adult safeguarding and sets out requirements for local authorities and partners to co-operate to perform their functions relating to care and support

Children Act 1989 - Section 17/47 set out requirements for partners to co-operate and share to ensure the provision of appropriate services for children in need, at risk or likely to be at risk

Children Act 2004 - Section 10 and Section 11 set out requirements for partners to co-operate and to safeguard and promote the welfare of children

Children and Families Act 2014 - Places duties on local partners to co-operate to support looked after children as well as children and young people with special educational needs or a disability

Health and Social Care Act 2012 - All health and adult social care organisations and service providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about individuals if the information is likely to facilitate the provision to the individual of health or adult social care services and sharing the information is in the person's best interest

4. WHAT INFORMATION WILL BE SHARED

Where Tier 3 Protocols are in place, these will detail specific information to be shared. Under the Tier 2 agreement information will be shared where it is necessary and lawful for the purposes set out above. The information will relate to:

- Children, young people, families and individuals whose personal data needs to be processed to enable the provision of social care or for other social care related reasons
- Their parents, carers, support network and family members
- Professionals who work with/support individuals in the activities referred to above

The information will include the following categories:

- Personal data as defined in the UK GDPR / DPA2018
- Special category personal data, including that relating to race, ethnicity, religion, sexuality and health (physical and mental)
- Criminal offence data (where processed with official authority or where a specific condition has been identified in Schedule 1 of the DPA 2018)

5. ROLES & RESPONSIBILITIES

Organisations will act as separate Data Controllers, processing for their own purposes. Where a party wishes to appoint a Data Processor to process the shared data, the organisation must ensure that this is agreed as part of this protocol, or as part of the Tier 3 protocol, and must ensure it is governed by a robust contract and detailed written instructions for processing.

6. INDIVIDUAL RIGHTS

As separate Data Controllers, organisations will be responsible for managing any rights requests made to them by following their own procedures.

7. INTERNATIONAL TRANSFERS

Shared personal data will not be transferred outside of the UK or EEA without the consent of the originating Data Controller and without the appropriate safeguards.

8. EXCHANGE OF INFORMATION

Data must be shared securely via secure email (Egress or TLS), or via other secure technical solutions which are approved for use by the organisations.

Further details will be provided in Tier 3 Protocols where these are in place.

9. DATA QUALITY

All information shared must be fit for purpose. Each originating signatory remains responsible for the accuracy of the data that they share. By signing this agreement, you are confirming that your organisation has the necessary processes and checks to ensure the accuracy of the information. You

should consider a process for issues arising from any partner receiving inaccurate data and ensure corrections are documented and cascaded to all Parties without delay.

10. SECURITY

All signatories will apply the appropriate technical and organisational security measures needed for the volume and sensitivity of the personal data being processed in accordance with the requirements of the DPA and UK GDPR and/or local practice commitments, such as the NHS Data Security and Protection Toolkit Standard. Specifically, you will:

- Ensure that your employees are appropriately trained to understand their responsibilities to maintain confidentiality and privacy
- Protect the physical security of the shared information in transit and at rest
- Restrict access to data only to those that require it, and take reasonable steps to ensure the reliability of employees who have access to data, for instance, ensuring that all staff have appropriate background checks, such as DBS.
- Maintain an up-to-date policy for handling personal data which is available to all staff
- Have a process in place to handle any security incidents involving personal data, including notifying relevant third parties of any incidents
- Ensure any 3rd party processing is agreed as part of this protocol and governed by a robust contract and detailed written instructions for processing.

11. MONITORING & REVIEW

All parties must agree to review this agreement every two years. If there is a data breach or major change to any of the signatory organisations they will undertake a review immediately.

12. DATA AND SECURITY BREACHES

In the case of any data or security breaches occurring that affect any data shared they must

- Be brought to the attention of the nominated officer in each organisation without delay and within 48 hours of the breach being detected and within 48 hours of the breach being detected
- Where the organisation in which the data or security breach occurred determines that the ICO needs to be informed the organisation should do so without undue delay and within 72 hours of the organisation becoming aware of the breach.

13. RECORDS, RETENTION & DISPOSAL

Data held will be reviewed and weeded as necessary. When no longer relevant, information will be destroyed by the party holding the information in accordance with their published records retention policy and confidential waste disposal policy.

Please check the following to confirm that your organisation commits to having the following in place:

- You agree to share this ISP with staff as necessary
- Privacy notices will be updated to include details of this data sharing
- Relevant written data protection and security policies are in place and regularly reviewed
- By signing you agree to the ISP being published (or a contact where the ISP can be easily requested).

14. WITHDRAWAL FROM THIS AGREEMENT

Any organisation can withdraw from the MAISP Tier 2 by writing to each partner organisation and giving 40 days' notice.

All information that has been shared or gathered under the Protocol will either be securely destroyed or will continue to be held in accordance with the Protocol agreement they were collected under.

It remains each organisations responsibility that the personal data is held in accordance with the law.

AGREEMENT

This agreement commences from the date it is signed.