**** 

**Surrey Multi-Agency Information Sharing Protocol (MAISP) Tier 3 - Agreement for data sharing for Children’s Multi-Agency Partnership**

**INTRODUCTION**

This data sharing agreement covers a range of activities undertaken within Surrey by the Multi Agency partnership which requires partner organisations to share personal data relating to individuals for the purposes of public protection and safeguarding. This Agreement forms a Tier 3 Data Sharing Agreement under the Surrey Multi Agency Information Sharing Protocol (MAISP).

This agreement does not constitute an overarching permission for the sharing of personal data. Rather, the agreement sets out the framework for the sharing of personal data between the parties as data controllers. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other. Any information shared under this agreement must be necessary, relevant and proportionate and must have a lawful basis.

**VERSION CONTROL**

| **Date issued** | **Version** | **Author** | **Approved by** |
| --- | --- | --- | --- |
| August 2024 | v1 | Fardowsa Ga’al | Nicole Miller |

**Date agreement comes into force:** 15/08/2024

**Date for review**: every 2 years

**Organisation Name:** Surrey County Council

**PURPOSE, SCOPE AND BENEFITS**

**PURPOSE**

The purpose of this agreement is to:

* Provide a framework for the sharing of personal data between the partners as data controllers. The agreement defines the principles and procedures that the partners will adhere to and the responsibilities that they owe to each other.
* Set out the lawful bases under UK GDPR and Data Protection Act 2018 through which the information is shared.
* Ensure all partners understand their responsibilities regarding information sharing.
* Facilitate a coordinated approach to the collection and sharing of relevant personal data between partners with respect and confidentiality, whilst safeguarding individuals’ legal rights.
* Promote trust between partner organisations and the public.
* Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
* Describe how this arrangement will be monitored and reviewed.
* Illustrate the flow of information from referral through processing and outcome.

**SCOPE AND BENEFITS**

This data sharing agreement covers information sharing between the members of the Surrey Multi-Agency Partnership (MAP) for the purpose of keeping children and young people in Surrey safe and protected from harm. Key legislation including the Children Act 2004 emphasises the need for the relevant partner agencies to carry out their duties around safeguarding and promoting the welfare of children and the importance of co-operation to improve the well-being of children in their area.

A key factor in many Serious Case Reviews has been a failure to record information, to share it, to understand the significance of the information shared, and to take appropriate action in relation to known or suspected abuse or neglect. Often it is only when information from a number of sources has been shared that it becomes clear that a child is at risk of, or is suffering, harm.

Information sharing can be vital to ensure that appropriate and timely decisions are made, that safeguarding partners are not working in silos and are able to carry out their statutory duties and public tasks to keep children safe and well.

**Role of the Children’s Single Point of Access (CSPA)**

All requests for support with a safeguarding concern for a child are made through Surrey Children’s Single Point of Access (CSPA). The CSPA plays a key role in evaluating the level of need and risk of incoming requests for support. The request will be reviewed by a Social Worker who will identify the best team to support based on the needs of the child/ren. In some instances, multi-agency checks are required to better understand the level of support required. CSPA activity concludes once assigned to the most appropriate team who support families or connect them to the most appropriate services.

**Role of the Multi-Agency Partnership (MAP)**

The MAP is a partnership of agencies, some co-located and others via virtual links, that have a duty to safeguard children and who have agreed to work within an integrated team to improve decision-making where there are concerns about a child. A co-located MAP team shares and analyses information from their agencies database in a safe, managed environment so that social work decisions on intervention can be made quickly and are based on the most accurate information available.

All information sharing decisions will be based on the Information Sharing Agreement and Guide, and information will not be shared other than in accordance with those documents. Decisions to share (or not share) information will be recorded and the record retained in the MAP. MAP co-locates safeguarding agencies and their data into a research and referral unit for notifications and referrals on vulnerable children. By doing this, MAP aims to identify and quantify risk and need by building a full picture on the child and their family.

The MAP is in place to assist in delivering the three key functions for the safeguarding partnership:

* **Information based risk assessment and decision making**

Identifying through the best information available to the safeguarding partnership those children and young people who require support or a necessary and proportionate intervention.

* **Victim identification and harm reduction**

Identify victims and future victims who are likely to experience harm and ensure partners work together to deliver harm reduction strategies and interventions.

* **Co-ordination of all safeguarding partners**

Ensure that the needs of all vulnerable people are identified and signposted to the relevant partner/s for the delivery and co-ordination of harm reduction strategies and interventions.

**Organisations covered by this agreement**

This agreement is for organisations who are members of the Surrey MAP:

* Surrey County Council, including Children’s Services and Education teams
* Police
* Health

The names of the organisations who have signed up to this agreement are published on the Surrey County Council MAISP pages at <https://www.surreycc.gov.uk/council-and-democracy/your-privacy/protocol-for-multi-agency-staff/signatories>.

**ROLES & RESPONSIBILITIES**

The partner organisations will each act as separate Data Controllers, processing for their own purposes. As signatories to the Surrey MAISP all partners have confirmed that they have the appropriate policies, procedures, training, vetting and security measures in place for compliance with data protection legislation.

**DATA PROTECTION IMPACT ASSESMENT (DPIA)**

The existing Data Protection Impact Assessment for the process of sharing information via the MAP has been reviewed and updated. This document highlights risk associated with the sharing. These include the risk of inappropriate sharing, as well as the risks around the storage of information. The DPIA is held by Surrey County Council and has been shared with the signatory agencies.

**PROPORTIONALITY**

Decisions on sharing personal information will be made on a case-by-case basis and with accordance to the principles of proportionality and necessity. Employees will use their professional judgment to weigh up the potential outcomes, considering both the consequences of sharing the information and the ramifications of withholding it. While the exchange of information may affect a practitioner's relationship with an individual or family; the safety of the child/young person must be the main consideration. There must be a lawful basis for personal information to be shared – see below – which are most likely to be for the purposes of safeguarding, for the prevention or detection of crime, with the consent of the individual or because the sharing is required or authorised by an enactment, a rule of law or the order of a court or tribunal.

**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 partner is responsible for ensuring that they process 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

Staff must consult their own organisation’s Data Protection Officer/Information Governance Manager and/or Caldicott Guardian if they are unsure or have any concerns about their lawful basis for processing personal data.

For the type of multi-agency working carried out by the MAP, where the partners have statutory duties to safeguard children, the lawful bases which are likely to be the most relevant are:

* Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject
* Article 6(1) (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
* Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

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”;

**Safeguarding** - Data protection law allows organisations to share information when required to identify children and individuals at risk of harm and to safeguard them from harm. Data protection law doesn’t prevent you from doing this. It simply helps you to share information in a fair, proportionate and lawful way. It can be more harmful not to share information that is needed to protect a child or a vulnerable adult who is at risk from neglect or physical, mental or emotional harm. The ICO provides guidance aimed at sharing information to safeguard children at <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/>.

**For the purposes of law enforcement by competent authorities**

The competent authorities under this agreement are generally (but not exclusively) police, probation services and youth offending teams.

The “law enforcement” purposes are defined in Section 31 of the DPA as “*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.*

**Consent**

The partners will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. This consent for involvement or actions is not the same however, must not be confused with the lawful basis of consent as a condition for processing personal data.

It is unlikely that it would be appropriate for public sector organisations to rely on the lawful basis of consent for using and sharing information under this agreement.

The Information Commissioner’s Office makes clear that:

 *“Consent will not usually be appropriate if there is a clear imbalance of power between you and the individual. This is because those who depend on your services, or fear adverse consequences, might feel they have no choice but to agree – so consent is not considered freely given. This will be a particular issue for public authorities and employers…* *If you are a public authority or are processing employee data, or are in any other position of power over an individual, you should look for another basis for processing, such as ‘public task’ or ‘legitimate interests’.”*

It is possible that some parties to this agreement, such as voluntary groups, may use consent as lawful basis for some personal data processing. Each partner is responsible for managing consent where they use consent as the lawful basis condition.

**Relevant legislation includes, but is not limited to:**

* Arrangements in regard of young people who may be deprived of their liberty such as the Deprivation of Liberty Safeguards or Liberty Protection Safeguards
* [Care and Support statutory guidance](https://www.gov.uk/government/publications/care-act-statutory-guidance/care-and-support-statutory-guidance)
* **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** – Section 107 of the Children and Families Act highlights the primary function of promoting and protecting the rights of children in England.
* Human Rights Act 1998 (Article 8)
* Criminal Justice Act 2003
* Crime and Disorder Act 1998 (Section 38, Section 115 and 117)
*Section 38 of the Crime and Disorder Act outlines the requirements of the local provision of youth justice services.*
* Care Act 2014 -
* Education Act 2002
* FGM Mandatory Guidance
* Health and Social Care Act 2012
* Localism Act 2011
* Mental Health Act 1983 and Mental Health Code of Practice
* Mental Capacity Act 2005 - Young people of 16 and 17 years old may fall within the remit of the Mental Capacity Act; Sections 2 – 4: Assessment of mental capacity and best interests decision making
* NHS Act 2006
* NHSE Safeguarding Vulnerable People in the NHS – Accountability and Assurance Framework 2015
* Police and Criminal Evidence Act 1984
* [Prevent Duty Guidance](https://www.gov.uk/government/publications/prevent-duty-guidance)
* [Working together to safeguard children 2023: statutory guidance (publishing.service.gov.uk)](https://assets.publishing.service.gov.uk/media/65cb4349a7ded0000c79e4e1/Working_together_to_safeguard_children_2023_-_statutory_guidance.pdf)

Additionally, the Caldicott Principles (below) should be applied to all information sharing:

Principle 1: Justify the purpose(s) for using confidential information

Principle 2: Use confidential information only when it is necessary

Principle 3: Use the minimum necessary confidential information

Principle 4: Access to confidential information should be on a strict need-to-know basis

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Principle 6: Comply with the law

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Principle 8: Inform patients and service users about how their confidential information is used

The following non-statutory guidance should also be read in conjunction with this agreement:

* [Information sharing advice for safeguarding practitioners - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice)

Other legislation that may be relevant when sharing information includes:

* Learning and Skills Act 2000
* Education (SEN) Regulations 2001
* Children (Leaving Care) Act 2000
* Immigration and Asylum Act 1999
* National Health Service Act 1977
* National Health Service Act 2006
* The Adoption and Children Act 2002
* The Localism Act 2011
* Welfare Reform Act 2012

**WHOSE DATA WILL BE SHARED**

Data Subjects will include:

* Children, young people and others who could receive support from children’s services
* Their parents, carers, support network and family members
* Individuals who have been convicted of offences against children and potential, suspected or alleged offenders
* Professionals who work with/support individuals in the activities referred to above

Deceased individuals

The sharing will involve data of deceased persons. Although this data will not be covered by data protection legislation it will still require due regard to the common law duty of confidentiality and the Human Rights Act.

**WHEN DATA MAY BE SHARED**

Under this agreement information will be shared only where it is necessary and lawful for the purposes set out above. The circumstances when information could be shared include:

* An individual (child, young person, service user, public or staff) is at risk of harm or likely to suffer harm
* A criminal offence has taken place
* It may prevent crime
* For the early identification, prevention or investigation of abuse or neglect (Section 47 Children’s)
* For investigations under Safeguarding Children Procedures
* To make an assessment of the service user’s needs so that an appropriate service can be provided
* To support work undertaken as part of the Health and Social Care prevention agenda
* To identify and plan for those who present a serious risk of harm to the public under the Multi Agency Public Protection Agreements (MAPPA)
* To aid decision making under the following schemes:
	+ Domestic Violence Disclosure Scheme
	+ Child Sexual Offences Disclosure Scheme
* To provide Onestop Surrey Notifications to other agencies
* Information to enable workers to undertake an assessment of needs
* To provide relevant data required for Safeguarding boards
* To provide data to support emergency incident plans
* To provide data required to meet any inspection regimes, timescales or requests
* Data required as part of the work on the Health and Social care prevention agenda
* Performance data
* Legitimate reason to make contact/confirm ID
* To facilitate feedback, training and improved practice

**WIDER SAFEGUARDING**

This agreement focuses on the sharing of information by the listed agencies. However, the partners all recognise that information is often provided to one or more of the agencies through referrals made by individuals, including members of the public, and by organisations not subject to this agreement. All partners are committed to keeping such information secure and protected, and only sharing this where it’s necessary, proportionate and lawful to do so and ensuring that they comply with the data minimisation principle.

**WHAT INFORMATION WILL BE SHARED**

Examples of the type of information that may need to be shared are below, however what needs to be shared will depend on the situation and will be on a case-by-case basis. The information shared must be necessary, relevant and proportionate and the receiving organisation must have a ‘need to know’. Anonymisation or pseudonymisation will rarely be possible because of the way the work focusses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

Data that can be shared includes but is not exhaustive:

* name, address and contact details
* age/date of birth
* ethnic origin, religion and other equalities information
* criminal information on allegations and convictions, police information and intelligence, information, anti-social behaviour (ASB) data
* school and educational information
* health records including NHS number, GP, Ambulance Services and other
* information on sex life and sexual orientation
* housing information
* children’s services information, referrals and assessments
* financial information
* images in photographs, film or CCTV
* employment information

**Constraints**

Information will not be shared where disclosure would prejudice ongoing criminal proceedings unless there is an overriding safety requirement to do so.

**ONWARD SHARING**

Any onward sharing must comply with specific conditions outlined by the original handler and any specific conditions agreed must be strictly followed. Moreover, the shared information cannot be used for any purpose beyond the scope outlined unless express consent is obtained from the original handler. This protocol ensures the integrity and lawful use of shared information while maintaining accountability and respect for privacy agreements.

**POLICE SAFEGUARDING REFERRALS**

Surrey Police Single Point of Access (PSPA) receive safeguarding referrals created by Surrey Police officers and staff.  PSPA will process these, screening them for potential sharing with Surrey Social services.  The decision as to whether it is necessary to share a referral or not, will be driven by mutually agreed guidance outside of this document (for example the current Level of Need Document or BRAG rating - this will be maintained and updated in accordance with any organisational requirements, development or learning).  As part of screening checks, PSPA will complete checks on EHM to establish if any child listed is currently an ‘open’ contact.  If there is information that a child is open, PSPA will commit to sharing every referral, even if it would not otherwise meet the criteria for sharing.

When PSPA decide to share a safeguarding referral with Surrey Social Care partners, PSPA will commit to providing full context around the incident.  It will contain information on the family unit as found by police AND/OR information on any other relevant parties (the suspect, involved neighbour, carer etc).  It may also include relevant other screening information relating to those parties (such as other risk assessments, for example DASH/DARA/HARA), as these often contain key information to inform risk management decisions.  It may also contain information around previous incidents, warning markers, intelligence or other information that is believed is relevant to the situation, or it is believed will assist partners.  The aim is to ensure that partners within the Multi-Agency teams have the all of the key information required to screen cases, make assessments and understand the incident in its entirety, eliminating the risk of missing something that could prove vital to safeguarding.  PSPA will only remove or redact information where it is clear and obvious that there is no value in its inclusion (for the purpose of safeguarding, providing context to the situation, or sharing operational safety information).  Practically, redactions will include situations such as persons not relevant to the situation (for example witnesses with no involvement), unnecessary personal data, non-factual opinion, or unrelated intelligence.

Surrey Police PSPA will share all referrals deemed necessary for sharing with Children’s Single Point of Access, unless there is information from EHM that the Child is currently an open contact.  In these cases they will be shared directly with the Social Services team currently shown as holding the case on EHM.  Surrey Police will ensure that the referral contains a rationale for sharing and is appropriately marked with handling instruction.  Surrey Police will aim to include contact details for the investigating officer, to allow partners to obtain further details and update directly.

As the data controller for the police referral (once shared), Childrens Social Care will have autonomy to decide where the Signs form, previously known as Single Combined Assessment of Risk Form (SCARF) is shared within Surrey County Council departments, in line with their own information governance processes and in order to carry out their lawful functions.  This may involve onward sharing of the whole referral, or redaction as necessary and appropriate.  Surrey Childrens services already have processes and policies in place that are suitable to govern the information sharing, as information is passed to secondary teams for review/assessment/action.

All partners to this agreement will abide by the handling instructions listed on the Signs form, and in particular will agree that the Signs form is not to be used for non-safeguarding processes without the express permission of Surrey Police (this includes but is not limited to use in legal and other court proceedings) and referring to Surrey Police prior to releasing information following a Subject Access Request.

Information that is shared with partners under this agreement is shared for the purposes of safeguarding and welfare. Any further use of this information by partners must be proportionate, lawful and in line with this purpose, and must take account of handling instructions as per the above paragraph on Signs forms. Information shared by partners with Surrey Children’s Services will be added to the relevant Liquid Logic system and will be held in line with the Council’s retention schedule.

**ACCESS TO PARTNERS’ COMPUTER SYSTEMS**

Police based in the Police Single Point of Access (PSPA) and Health colleagues have **read only** access to the Council’s EHM system for the purposes of accessing up to date information in order to make informed decisions relating to the activities covered in this agreement.

* The Police PSPA team are collocated with Children’s Services CSPA team. PSPA have read only access to the Council’s EHM system so that they can identify whether children are already open to Children’s Services and so that they can complete MAPEs.
* Health Advisors who are co-located in MAP have been given access to EHM for completion of MAPEs
* Health and Police colleagues’ access to EHM is set to the ‘External Partner’ profile
* Any additional access must be approved by the SCC Sponsor (C-Spa Service Manager) and go through the SCC approval process (IG, Caldicott and IT&D)

Police and Health colleagues will access EHM using their own organisation’s devices once they have received the appropriate training. They must abide by the same requirements around security, confidentiality and data protection, including annual IG training, as the Council’s staff and equal to their use of Health/ Surrey Police Systems outlined in their own organisation’s policies.

The use of data for any other purpose from EHM must be requested with express permission from Surrey County Council, this will be reviewed and a decision made. At this time all required documentation will be completed.

Children’s Services MAP staff have no access to health, police or probation systems – they must request information from the partners with either the permission of the individual in question or an appropriate lawful basis and rationale for overriding the need for permission.

**DATA PROCESSORS**

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.

**INDIVIDUAL RIGHTS**

As separate Data Controllers, organisations will be responsible for managing any rights requests made to them by following their own procedures. When responding to subject access requests or other disclosure requests, organisations must ensure that they follow the guidance above under **Constraints, Onward sharing** and **Police safeguarding referrals** and liaise with the originating organisation where applicable.

**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.

**EXCHANGE OF INFORMATION/ HOW INFORMATION IS SHARED**

Information should always be shared securely, either by a secure IT connection, encrypted email, or other secure technical solution approved for use by the organisations or via a secure and tracked transfer of paper documents. Information should never be sent via a non-secure method. The employee/organisation sending the information must chose the most appropriate method of transfer and be responsible for its safe delivery.

**Surrey County Council** – all emails containing sensitive data must be protectively marked and will then be automatically sent securely using either TLS or Egress. Emails sent via TLS will be automatically encrypted during transit. Emails sent via Egress will either be encrypted in transit or additionally will remain encrypted on delivery (depending on the option chosen by the sender).

To reduce the likelihood of data breaches, all individuals should avoid using pre-populated information when sending emails.

**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.

**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.

**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.

**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 appropriate supervisor n 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.

The organisations should provide reasonable assistance as is necessary to each other to facilitate the handling of any data security breach, or a dispute or a claim brought by a data subject or by the Data Protection Authority.

**BUSINESS CONTINUITY**

Each partner is required to have a robust business continuity plan and process in place.

**RECORDS, RETENTION & DISPOSAL**

Personal data held by partners should be regularly reviewed and securely destroyed in accordance with their own 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 as necessary 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).

**WITHDRAWAL FROM THIS AGREEMENT**

Any organisation can withdraw from this agreement 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 organisation’s responsibility that the personal data is held in accordance with the law.

**AGREEMENT**

This agreement commences from the date it is signed.