Data Sharing Agreement - Risk Outside The Home (ROTH)

1. Introduction to the data sharing agreement

This data sharing agreement(DSA) documents how the parties to this agreement, listed in Appendix A will share data about children and families for safeguarding purposes. By signing this Agreement, the named agencies agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This agreement has been developed to:

- Define the specific purposes for which the signatories have agreed to share information.
- Outline the personal and special category data to be shared.
- Set out the lawful basis conditions under UK GDPR and Data Protection Act 2018 through which the information is shared, including reference to the Human Rights Act 1998 and the Common Law Duty of Confidentiality.
- Stipulate the roles and structures that support the processing and exchange of information between the parties.
- Describe how the rights of data subject(s) will be protected as stipulated under data protection legislation.
- Describe the security procedures necessary to ensure that compliance responsibilities under the data protection legislation and party specific requirements, and
- To illustrate the flow of information from referral through processing outcome.

The parties to this agreement cannot amend or add appendices unless agreed as part of a formal review. It is expected that each party will have procedures, processes and policies sitting underneath this agreement, for their respective organisations. These will, for example, describe the specific processes for secure transfer of data.

Document Version	Version 1
Author/Owner	Caroline Ash, Head of Conferencing and Review, Achieving for Children
Date first published	1 September 2022
Date of last review	
Date of next review	31 August 2024

1.2 Responsibilities of the parties involved

The parties are registered Data Controllers under the Data Protection Act. All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights & complaints,
- identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.
- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.
- Parties and their staff must consult the organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian if they are unsure at any point in the processing and sharing of personal data.

1.3 Assessment and review

A review of the data sharing agreement will take place every two years, unless otherwise agreed by the parties' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not slipped, the benefits to the data subjects and parties are being realised, and the procedures for information security are effective.

1.4 Termination of agreement

In the event of a termination of this agreement, each party may continue to hold information originating from other parties for which they are data controller.

2. Purpose and benefits

There has been growing professional understanding of the harm to a child that occurs outside of the family, takes place in spaces within the community and typically from someone who is not a family member. This is more widely known as contextual safeguarding and exploitation.

Where this harm is significant, these worries would usually lead to a child protection

conference and plan, however the feedback from families in the boroughs of Kingston and Richmond is that the child protection process is unhelpful when the worries are outside the home. An 18 month pilot on behalf of Kingston and Richmond Safeguarding Children's Partnership (KRSCP) led to the development of the ROTH framework which is better suited to address risk outside the home.

ROTH is a multi-agency response which sits within the safeguarding umbrella and the review meetings are equivalent to a child protection conference but operates outside of the Multi-agency Safeguarding (MAS) data sharing agreement.

The children supported through ROTH are at significant risk of harm through contextual risk and exploitation, including criminal exploitation and sexual abuse. Information necessary for safeguarding decisions in relation to children and young people is held by numerous statutory and non-statutory agencies. To deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need the full information concerning a child and their circumstances to be available to them.

2.1 Benefits

The benefits of this DSA are:

- Strengthens collaborative plans for children better reducing extra familial risk.
- Enables professionals to be more responsive in identifying who is best placed to provide specific support for the child.
- ROTH plans are SMART, multi agency and thoughtfully created
- Removes barriers to effective information sharing
- Coordinated and consistent response to safeguarding concerns
- Improves outcomes for children and young people at significant risk outside the home
- Families feel more engaged in safeguarding their children

2.2 Principles of data sharing

Effective data sharing is a vital element of both early intervention and safeguarding of children and young people at risk of harm outside the home. Organisations can hold different pieces of information which need to be placed together to enable a thorough assessment and plan to be made.

To share information, a lawful basis for doing so must be identified. This may come from legislation or from statutory guidance such as Working Together to Safeguard Children 2018 which places responsibilities on organisations outside of the Partnership such as private organisations, sports clubs, voluntary, community and faith sectors.

The sharing of personal data must comply both with the UK GDPR data protection principles and the Caldicott principles listed at Appendix B.

2.3 Lawful basis for sharing

The sharing of information must comply with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements. This is a complex area and each Partner must take their own decisions and seek advice from their organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian.

For purposes other than law enforcement by competent authorities

Articles 6, 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below.

Article 6(1) - personal data processing

(c) processing is necessary for compliance with a legal obligation to which the controller is subject

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.

(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.

Article 9(2) - special category personal data processing

(c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Use of this article requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 is met. For this agreement these are:

- *statutory and government purposes under Para 6(1)(2)*
- *Preventing or detecting unlawful acts under Para 10(1)(2)(3)*
- *Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)*

For the purposes of law enforcement by competent authorities

The "competent authorities" are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under this agreement are generally (but not exclusively) Metropolitan Police, youth offending teams and government departments.

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".

There are additional safeguards required for "sensitive processing". This is defined in Section 35(8) as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
(c) the processing of data concerning health;
(d) the processing of data concerning an individual's sex life or sexual orientation.

The additional requirements are given in Section 35(4) and (5). Both require an appropriate policy document, and this document will form part of the policy for such processing, although competent authorities will need to satisfy themselves that their own internal policy documents fully cover such use.

Section 35(4) requires the consent of the data subject, 35(5) requires that the processing be strictly necessary for the law enforcement purposes, and meets a condition in Schedule 8. For the processing in relation to the purposes here, the following conditions in Schedule 8 are met:

- Statutory etc. purposes Para 1(a)(b);
- Administration of justice Para 2;
- Protecting individual's vital interests Para 3;
- Safeguarding of children and of individuals at risk Para 4(1)(2)(3)(4);

The applicable legislation that provides the lawful basis is listed in more detail in Appendix C - Applicable legislation

2.4 Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) or explicit consent (Article 9 (a)) as the lawful basis conditions used for processing under this agreement.

Consent is not generally the lawful basis public sector organisations use for processing information shared under this agreement. It is possible that the other parties, such as voluntary groups, may use consent as a lawful basis for some personal data processing. Each party is responsible for managing consent where they use consent as the lawful basis condition.

2.5 Proportionality and necessity

Proportionality and necessity are factors to be taken into consideration when deciding whether to share personal information. In making the decision, employees must weigh up what might happen as a result of the information being shared against what might happen if it is not, and apply their professional judgement.

Although sharing of information can impact on a practitioner's relationship with an individual/family, keeping the child safe must always be the first consideration. Safeguarding is a "special purpose" under the Data Protection Act and as such you should share if the sharing is necessary for the protection of an individual, under or over 18, who is at risk of significant harm.

You are expected to justify that you believed sharing was necessary for one of the following criteria:

- necessary for the purposes of preventing or detecting crime
- required or authorised by an enactment, by a rule of law or by the order of a court or tribunal
- in the particular circumstances, was justified as being in the public interest.

Or that you acted in the reasonable belief that:

- the person had a legal right to do the obtaining, disclosing, procuring or retaining
- the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or

2.6 Other relevant legislation

The actual disclosure of any personal data to achieve these objectives must also be conducted within the framework of the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence. Caldicott Principles also apply to all information sharing and they are listed in Appendix B: Data Protection & Caldicott Principles.

- Human Rights Act 1998 (HRA)
- Common law duty of confidentiality
- Confidentiality and sharing for direct care

2.7 Freedom of Information

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also

allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who holds the information (data controller).

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Each party agrees that they have undertaken a DPIA (Data Protection Impact Assessment), where they feel the processing meets the legislative criteria for a DPIA.

3.1 Right to be informed - privacy notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of the UKGDPR and will issue appropriate notices which inform the data subject that the information will be shared with the parties under this agreement.

In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware.

3.2 Data subject rights requests and complaints

Each organisation must have in place appropriate policies and processes to handle data subject requests made in line with data protection law, to ensure they are responded to

within deadline and in an appropriate manner. Requests include; right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision making including profiling.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties where relevant and appropriate. In each case each party is responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair and objective complaint procedures. Any complaints from individuals about how their data is being processed or shared will be handled under the policy and processes of the organisation concerned.

3.3 Data subjects

The data subjects whose data is shared under this agreement include the following:

- Child
- Family members, carers and other persons whose presence and/or relationship with the child is relevant
- professionals e.g. social worker, EWO
- actual or suspected perpetrators or witnesses

4. Data

Information will include:

- **Personal and special category** to enable the identification and reduction of risk and harm to children.
- **Aggregated (anonymised or pseudonymised)** data reporting to enable the full extent of risk to children by individuals and groups to be explored whilst protecting sensitive information.
- **Aggregated (anonymised or pseudonymised)** and personal data regarding employees in relation to serious case reviews, investigations into allegations against staff, learning review and workforce development.
- **Personal and anonymised data** required for statutory returns.

4.1 The data to be shared

Due to the complexities in safeguarding children, providing a prescriptive list of data fields to be shared is difficult. Not all the information will be shared on a case by case where an organisation has a “need to know” the information.

Data that can be shared includes:

- name and contact details
- age/date of birth
- ethnic origin, religion and other equalities information
- school and educational information
- social services information, referrals and assessments
- images in photographs, film or CCTV
- employment information
- criminal information on allegations and convictions, police information and intelligence
- health records including NHS number
- information on sex life and sexual orientation
- housing information

4.2 Confidential information

In this agreement, we refer to personal data, as defined by data protection legislation. However, the word 'confidential' may be used by individuals and practitioners to describe information and can mean different things to different people.

Confidential can mean:

- Personal and special category data as defined by data protection legislation
- Patient Identifiable Information (PII) or 'personal confidential information'; both terms most commonly used in health settings
- Information which is not already lawfully in the public domain or readily available from another public source
- Information that has been provided in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

4.3 Storing and handling information securely

Information should only be stored and shared in accordance with data protection legislation and follow information security policies and procedures of the relevant organisation.

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

Email is not generally a secure method of transferring personal data. It would be prudent for parties to establish whether there are any encrypted paths between them, and write that into the organisation's processes for employees. In the absence of that, secure email systems

such as Egress and Encrypt and Send must be used. Description of specific transfer processes must be in relevant process documents within each organisation.

Information may be shared over the phone, in a virtual meeting, or a face to face meeting. Employees must ensure that attendance and distribution of content is limited, with minutes or recordings with limited distribution. Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable

Any paper records printed must be kept to a minimum and kept secure at all times whether in the office, home or during transit. Organisations must adopt an appropriate policy surrounding the use and transfer of paper records. Appropriate security methods must be applied when storing or disposing of paper records.

4.4 Access controls and security

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All personal data held electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted.

Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer.

There is an expectation that partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security.

4.5 Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that suitable written agreements are in place, and that appropriate due diligence has been completed for the transfer of data.

4.6 Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality. Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.

4.7 Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This must include assessing the level of risk to the data subject(s), as well as to make a decision on notifying the ICO within the statutory time frame of 72 hours. This complies with Articles 33 and 34 of UK GDPR.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed and appropriate coordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the partner's internal disciplinary procedures. If misuse is found there should be a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.8 Data retention and disposal

Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.

Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.

Appendix A -Key parties to this agreement:

Organisation	Signatory	Signature	Date signed
Kingston and Richmond Safeguarding Children's Partnership			
Achieving for Children			
Metropolitan Police			
NHS South West London Integrated Care Board			
Substance Misuse Partner			
Kingston Adult Social Care			
Richmond Adult Social Care			
Local voluntary groups			
Kingston Housing			
Richmond Housing			

Appendix B - Data Protection & Caldicott Principles

The Principles as described in Article 5 of the General Data Protection Regulation

1) lawfulness, fairness and transparency	processed lawfully, fairly and in a transparent manner in relation to the data subject
2) Purpose limitation	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3) Data minimisation	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4) Accuracy	accurate and where necessary, kept up to date. Inaccurate data must be erased or rectified without delay
5) Storage limitation	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6) Integrity & confidentiality	secured through appropriate technical or organisational measures, including protection against unauthorised or unlawful process

The Caldicott Principles

1) Justify the purpose(s) for using confidential information	Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.
2) Use confidential information only when it is necessary	Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.
3) Use the minimum	Where use of confidential information is considered to be

	necessary confidential information	necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function
4)	Access to confidential information should be on a strict need-to-know basis	Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes
5)	Everyone with access to confidential information should be aware of their responsibilities	Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.
6)	Comply with the law	Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law
7)	The duty to share information for individual care is as important as the duty to protect patient confidentiality	Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.
8)	Inform patients and service users about how their confidential information is used	A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include

	providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Appendix C - Applicable legislation

The Children Act 1989	Under S.47 of the Children's Act 1989, a Local Authority has a duty to investigate when informed that a child in their area is in police protection or the subject of a protection order. This regulation provides specific powers giving a legal basis under Section 8 of the DPA for this use.
The Children Act 2004	The Children Act 2004, as amended by the Children and Social Work Act 2017, places duties on key agencies in a local area. Specifically, the police, clinical commissioning groups and the local authority are under a duty to make arrangements to work together, and with other partners locally, to safeguard and promote the welfare of all children in their area. This regulation provides a general safeguarding and welfare power giving a legal basis under Section 8 of the DPA for this use
The Crime and Disorder Act 1998	Each LA in England & Wales has the responsibility to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this.
Working Together to Safeguard Children 2018	Local authorities, working with partner organisations and agencies, have specific duties to safeguard and promote the welfare of all children in their area. The Children Acts of 1989 and 2004 set out specific duties: section 17 of the Children Act 1989 puts a duty on the local authority to provide services to children in need in their area, regardless of where they are found; section 47 of the same Act requires local authorities to undertake enquiries if they believe a child has suffered or is likely to suffer significant harm. This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for national bodies.

London Child Protection Procedures 2020	The London Child Protection Procedures sets out the procedures which all London agencies, groups and individuals must follow in identifying, raising and responding to welfare concerns when coming into contact with or receiving information about children 0 to 17 years, including unborn children and adolescents up to their 18th birthday This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for various London bodies.