Data/Information Sharing Agreement – Supporting Families

Contents

1. Introduction to the Data Sharing Agreement

This Data Sharing Agreement [DSA] documents how the parties to this agreement will share data.

Information about the data subjects is only shared where it has been identified that they are eligible to receive support for the supporting families scheme under the Department of Levelling Up, Housing and Communities (DLUHC) Supporting Families Framework and stipulated within the DLUHC approved outcomes plan.

The key agencies are listed in Appendix A, and the agreement is to be signed by all relevant parties, including local partners, voluntary sector, and any specialist organisations.

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 signatory agencies have agreed to share information.
- Outline the Personal, Special Category and Criminal 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 procedure that will support the processing/sharing of information between agencies.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

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.

1.1. Ownership of this agreement

This agreement was drafted by a working group of representatives of the police, local authorities and London Councils. These professionals were specialists in the troubled/supporting families programme, police procedures, information governance and law. The local authority representatives worked under the banner of the Information Governance for London Group (IGfL), to draft one agreement that would work for all boroughs and Metropolitan Police BCUs across London, and the City of London Police. The aim is to reduce the number of versions of sharing agreements that historically differed between boroughs, partly to reduce the burden on pan-London organisations that must have agreements with multiple boroughs.

IGfL, a group of information and security professionals at London boroughs, assisted with coordination of this agreement, but the responsibilities within it, and compliance with data protection legislation, remain with the listed Data Controllers. The term 'police' refers to both the Metropolitan Police Service and the City of London Police.

1.2. Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act. Signatories are identified as those who have signed this agreement on the Information Sharing Gateway. A list of expected types of signatories is at Appendix A.

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.

Organisations 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. Confidentiality and vetting

Each Partner must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality.

Each Partner must ensure that suitable vetting has taken place. This may be through standard employee checks (BPSS or equivalent), DBS, Security Vetting or Counter Terrorist Check [CTC].

1.4. Assessment and review

A review of this information sharing agreement will take place after an initial six months and yearly thereafter, unless otherwise agreed by the organisations' 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 organisations are being realised, and the procedures followed for information security are effective.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise, as will any changes to the signatory parties.

The working group who drafted this agreement strongly recommends that a working group approach is used for any reviews, as this was a successful way to achieve pan-London and cross-specialism consensus to one sharing agreement.

1.5. Termination of agreement

In the event of termination of this agreement each party may continue to hold information originating from other parties for which they are the Data Controller.

1.6. Outside of this agreement

There are multiple other information sharing arrangements that form part of the duties of the parties and involve similar data for often similar overall purposes, like safeguarding and preventing crime. A non-exclusive list is below. Some of these DSAs are live and others are still in draft.

It should be noted that only the data specified in this DSA is covered by this particular DSA. The lawful basis specified, the Digital Economy Act Act 2017 (see Appendix C), has particular requirements attached to it. Other information will be shared between councils, the Police, and other partners which is used for wider purposes including safeguarding, family interventions, and similar work, and which may be undertaken by teams in councils undertaking troubled/supporting families type work. This will be covered in other DSAs as listed in the table below. That is not included in this DSA which is specific and limited in scope.

Area of work	Description

ASB	The sharing of data regarding anti-social behaviour and related enforcement
Adult Safeguarding	Sharing information to prevent and deal with all types of abuse against adults, including issues such as financial abuse and cuckooing.
MAPPA - Multi-Agency Public Protection Arrangements.	Information sharing between probation, police, councils and other agencies as mandated under MAPPA for the most serious risk posing offenders
Prevent/Channel Panel	The PREVENT strategy and Channel Panel are aimed at reducing the risk of radicalisation of young persons
Rescue & Response (County Lines)	The exploitation of persons to sell and move drugs between areas, commonly known as “county lines” is a major element of modern exploitation of young persons and in some cases, modern slavery.
IOM	Integrated Offender Management (IOM) tackles the most prolific reoffenders and those who commit offences deemed to have the most significant impact on the local community.
MAS/MASH	The multi-agency safeguarding DSA covers children’s safeguarding, well-being, and MACE sharing.
Licensing	This covers sharing for all licensing including alcohol, gambling, special treatments and sexual entertainment venues, and various other areas such as pet shops and highways licenses
Gangs/Serious Youth Violence (SYV)	The gang and serious youth violence projects are part of specific police-led initiatives. There are 2 agreements: one councils/police, and one council to council.
Residual crime	A local BCU signed DSA to cover lower level crime not covered in other DSAs such as caution registers, nuisance, and other criminal issues.
Domestic Abuse Multi-Agency Risk Assessment Conference (MARAC) and Violence Against Women and Girls (VARG)	Domestic abuse and violence against women and girls have complex roots, and as such commonly involve police, social care, health, voluntary and faith organisations in case management.
Youth Offending	Collaborative approaches to preventing offending and re-offending by children.
CCTV	The sharing between councils and police of CCTV footage, whether live feed or recorded, and from any type of device including cameras, drones and vehicle CCTV

Environmental Crime	There are two agreements, one between councils and the Environment Agency covering crime that the EA handles, the other is between councils for a wider range of environmental related crime such as fly-tipping, dog fouling etc
Trading Standards	This covers information sharing between the police and National Trading Standards London Region, and between the police and local councils for the whole range of trading standards related activity such as scams, rogue traders etc
People affected by an emergency	Sharing between agencies including councils, police, and London Ambulance and London Fire and Civil Defence Authority to handle the immediate and longer term response to emergencies such as floods, civil disturbances, attacks etc

2. Purpose and Benefits

To deliver the best decisions that ensure timely, necessary and proportionate interventions, decision makers need the full picture concerning an individual and their circumstances. This data sharing agreement aims to support and improve the welfare of families by identifying those with multiple complex problems and addressing their needs through systemic joined up working and intervention.

See section 1.6 above which explains the limited scope of this DSA and that other information relevant to practitioners in this area is likely to be shared between agencies under different DSAs. This DSA covers only the personal data described in section 4. However, practitioners will find they receive and share additional personal data from and with other agencies relating to families under other DSAs.

Information viewed alone or in silos may not give the full picture or identify the true risk. All the information from various agencies needs to be available and accessible in one place; to keep local residents and other stakeholders safe and assist signatories to this Agreement in discharging their obligations under the Act and other legislation. Data sharing will enable the parties to use analytical techniques to identify families who are most at risk, vulnerable or likely to have negative outcomes. This means informed decisions can be made to target limited resources, which will allow the parties to facilitate enhanced assistance to the mutual benefit of families and public services as part of a prevention strategy.

Proactively introducing this support to families encourages more positive outcomes and prevents the use of crisis services and long-term poor outcomes. This allows families to be more self-sustaining and less reliant on the state. The support provided aims to achieve “significant and sustained progress” with the families and prevent households from being drawn into different types of crime like anti-social behaviour,

domestic violence and abuse. Progress is determined locally with key stakeholders in line with DLUHC Guidance.

2.1. Benefits

The benefits of this DSA are to:

- Cover the sharing of information for the purposes set out in section 2.
- Remove barriers to effective information sharing.
- Sets parameters for sharing personal data and clearly identifies the responsibilities of organisations.
- Identify the correct lawful basis to share personal information.
- Ensure information is shared whenever there is a requirement to do so.
- Enables authorities to share data on performance, quality assurance, learning and impact analysis.
- Raises awareness amongst all agencies of the key issues relating to information sharing and gives confidence in the process of sharing information with others.
- Greater efficiencies in processes and resources.
- Preventing and detecting crime.
- Facilitate provision of proactive support for eligible families
- Assist with improving long-term outcomes for residents
- Strengthen resident autonomy
- Aid future planning

2.2. Principles of information sharing

Effective information sharing is a vital element of both early intervention and safeguarding of children and young people at risk of harm or neglect. 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 or the Children Act 2014, which places responsibilities on organisations outside of the Partnership such as sports clubs, private organisations, and the voluntary, community and faith sectors.

The sharing of personal data must comply with both the GDPR Principles and the Caldicott Principles, listed at Appendix B. Together, those principles lead to a series of questions and considerations to be answered before sharing takes place. These are listed as an Information Sharing Checklist in *Appendix D: Information Sharing Checklist.*

2.3. Lawful Basis

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
(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 Use of this article requires that the Data Protection Act section 8 be satisfied. The laws given at Appendix C – Applicable legislation provide for each party a legal basis under section 8 – the specifics are noted in the appendix.

Article 9 (2) – Special Category Personal Data Processing: It is not anticipated that special category data will be shared under this DSA.
It is not anticipated that special category data will be shared under this DSA. However if it is then the legal basis will be Article 9(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 etc., and government purposes under Para 6(1)(2)* ● *Preventing and detecting unlawful acts under Para 10(1)(2)(3)* ● *Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)*

Art. 10 GDPR : Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. The art 6 legal basis is above.

The Data Protection Act 2018 Schedule 1 condition:

Part 1 para 2(1) Health or social care purposes: This condition is met if the processing is necessary for health or social care purposes… (e)the provision of social care

Part 2 para 6 Statutory etc and government purposes: 6(1) This condition is met if the processing—
(a)is necessary for a purpose listed in sub-paragraph (2), and
(b)is necessary for reasons of substantial public interest.
(2) Those purposes are—
(a)the exercise of a function conferred on a person by an enactment or rule of law;
Preventing or detecting unlawful acts

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) 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.

It is not anticipated that such information will be shared under this DSA. However, if it should be then 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 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);

In order for competent authorities to carry out and share sensitive personal data with partners:

that processing must be strictly necessary; and

at least one condition specific in Schedule 8 of the DPA be satisfied. An analysis of three relevant conditions is set out below:

Strict necessity

Although it is difficult to anticipate all the circumstances in which sharing under this agreement may be necessary, in general competent authorities do not consider that there are any other less intrusive means of obtaining personal data held by partners.

The reasons for the necessity of sharing personal data is set out in Sections 2 and 2.1 (above) and 2.6 (below).

Schedule 8 conditions

The following conditions set out in Schedule 8 of the DPA 2018 are likely to be satisfied, depending on the precise context of the data processing:

Paragraph 1: Statutory etc purposes

This condition is met if the processing—

(a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and

(b) is necessary for reasons of substantial public interest.

The processing of the data is carried out in the exercise of the legal powers and duties of the Police. It is plainly in the substantial public interest that for example witness, victims and potential suspects are located as soon as reasonably practicable by the police.

Paragraph 3: Protecting individual's vital interests

This condition is met if the processing is necessary to protect the vital interests of the data subject or of another individual.

This condition is met in cases where there is a risk to the life of the of the data subject or where the data subject poses a threat to the life of either his or herself or the life of others. This may be the case where the police consider that a victim faces an ongoing risk of harm.

Paragraph 4: Safeguarding of children and of individuals at risk

(1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.

This condition is met where the child or vulnerable adult is at risk of harm (whether physical or mental), and the police are unable to obtain consent for any of the reasons listed in para 4(2). This condition will be met in most cases given the serious risk of harm posed to missing children or vulnerable adults in the aftermath of a major incident.

The terms of this agreement address the requirements for data sharing pursuant to Part 3 of the DPA 2018.

To note that there is a separate regime for intelligence service processing, which falls outside the remit of this DSA.

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 the 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.

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.

2.7. Common Law Duty of Confidence

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children.

However, for the police, as a safeguard before any information is passed on, it will undergo an assessment check against criteria (included in Child Abuse Investigation Command Standard Operating Procedures) by the Public Protection Desk (PPD). Whilst still applying proportionality and necessity to the decision, the protection of children or other vulnerable persons would clearly fulfil a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim.

Information held by other agencies may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure as information can be shared where there is a strong enough public interest to do so.

When overriding the duty of confidentiality, the parties may seek the views of the organisation who hold the duty of confidentiality and consider their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

2.8. 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). In order to ensure that the authority in receipt of the FOIA request is able to respond within the statutory deadline, any request for assistance or information made to partner authorities should be made and processed within two working days, and any data exchange completed within seven working days.

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

Organisations that rely on the Digital Economy Act are obligated to publish the Data/Information Sharing Agreement, Data Protection Impact Assessment, Security Plan and Business case.

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.

For organisations relying on the Digital Economy Act 2017, a business case and security plan are highly recommended, as stated in the Code of Practice.

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 the 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

There is a breadth of data subjects whose data is shared under this agreement. The data subjects include the following:

- child
- family members, parents, carers and other persons whose presence and/or relationship with the child, is relevant to identifying and assessing the risks to that child
- victims
- actual or suspected perpetrators
- professional adviser or consultant (eg doctor, lawyer, employment advisors)

Many of the data subjects are vulnerable. Parties to this agreement are in positions of power over data subjects and data subjects have little or no control over why and how their data is processed.

4. Data

The personal data and its processing involved in these workstreams is extensive, highly sensitive and at times intrusive. There is a high volume of data and data subjects. Anonymisation or pseudonymisation will rarely be possible because of the way the work focuses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

Information will include:

- **Personal and criminal data** to enable the work with families requiring assistance under the supporting families programme work in the borough
- **Personal and criminal data** for law enforcement purposes,
- **Aggregated (anonymised or pseudonymised) data** reporting to enable the programme to further understand the safeguarding priorities.

4.1. The data to be shared

Due to the complexity of the work involved in the subject of this DSA, providing a prescriptive list of data fields to be shared is difficult. Not all the above information will be shared in every case; only relevant information will be shared on a case-by-case basis where an organisation has a ‘need-to-know’ the information.

Data that will be shared includes:

- Name and Contact details
- Age/date of birth
- Whether data subject is involved in or convicted of a crime
- The quarter that involvement/conviction took place
- Whether the data subject is a victim or perpetrator
- No special category data is expected to be shared. However in a very small minority of cases racial or sexuality data may be shared where the child requires support over these issues

4.2. Deceased persons

It is noted that the sharing may involve data of deceased persons. This data will not be covered by data protection legislation but will still require due regard to the common law duty of confidentiality and the Human Rights Act.

4.3. 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.

4.4. Storing and handling information securely

IInformation must be stored and shared lawfully and securely. Special category data may need a higher level of security. The employee/organisation sharing the information must choose the most appropriate secure method of transfer and be responsible for its safe delivery.

Electronic records:

Organisations may have different electronic methods for storing and sharing information securely. Some have local restrictions which block access to information shared using specific tools.

Parties must make sure the chosen method is suitably secure and that access is only provided to those who need it, and only to the data needed.

Unencrypted email (i.e. sent in plain text over the public internet) must not be used to share information under this DSA.

Sharing methods that may be appropriate include:

- **Email encryption tools** where the email and attachments are encrypted from named sender to named recipient (e.g. Microsoft 365 Message Encryption; Egress Protect)
- **Encryption via Transport Layer Security** (TLS) where the email and attachments are encrypted in transit over the internet. Both the sender and recipient email domains must have TLS enabled. This can be checked using https://www.checktls.com/
- **Secure corporately managed data repository and sharing platforms** (e.g. MS Teams; Google Docs)
- **Secure group email services** (e.g. CJSM: https://cjsm.justice.gov.uk/index.html)
- **Secure File Transfer Protocols**
- **Virtual Private Networks**

The above are examples: get advice from your organisation's information security or IT teams on secure methods of sharing available at your organisation and document these in the organisation's process documents.

Phone/virtual meetings/face-to-face meetings:

Information may be shared over the phone, in a virtual meeting, or at face to face meetings. Meeting attendance and distribution of content, e.g. meeting minutes or recordings, must be limited to those with a need to know.

Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable.

Individuals should be aware of their surroundings and the presence of other individuals or voice recognition or 'Internet of Things' devices (e.g. virtual assistant apps like Alexa, Cortana, SIRI) to ensure they aren't overheard by those that should not have access to the information discussed.

Paper records:

Printed paper records must always be kept to a minimum and kept secure 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.

4.5. 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 by partner organisations 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.

4.6. Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that appropriate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. These are for example, a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, and/or standard data protection contractual clauses[

4.7. 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.

4.8. 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, and Section 67 and 68 of the DPA 2018 for personal data processed for law enforcement purposes.

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.

4.9. Retention & 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.

5. Signatures

Parties other than the Metropolitan Police will sign on the Information Sharing Gateway

This agreement is signed on behalf of The Metropolitan Police

……

Name and Rank Date

Version control	
Document production date	March 2022

Document currency	Final 1.0

6. Appendix A : Parties to this agreement

Organisation	Duties
London Borough Council	● Facilitating the Supporting Families Scheme ● Co-ordinating, gathering, processing, personal information held about the family known to the local authority in conjunction with information received from partner agencies to identify vulnerabilities within the framework ● Creating partnerships to ensure that the families receive the support that they require ● Putting support plans in place to help reduce concerns
Metropolitan Police Service and City of London Police	● Co-ordinates, gathers, processes, risk assesses and shares police information relevant to public protection, missing children, cse, child protection (MERLIN), domestic violence, gang and county line related information ● Supports assessments of risk and vulnerability

7. Appendix B: Data Protection & Caldicott Principles

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

1) Fair & Lawful
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 processing and against accidental loss, destruction or damage.

7) Accountability
processed by organisations that take responsibility for the personal data, with appropriate measures and records in place to demonstrate compliance.

The Caldicott Principles

Principle 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.

Principle 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.

Principle 3
Use the minimum necessary confidential information
Where use of confidential information is considered to be 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.

Principle 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.

Principle 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.

Principle 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.

Principle 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.

Principle 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. As a minimum, this should include providing accessible, relevant and appropriate information. In some cases, greater engagement will be required.

8. Appendix C: Applicable legislation

All legislation is available at www.legislation.gov.uk

Legislation	Main purpose of Legislation
Digital Economy Act 2017 part 5 and associated codes of practice	The Act allows for public sector data sharing in various circumstances including for achieving the aims of the troubled and supporting families programme as detailed in the codes : https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice
Children Act 1989	Under S.47 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.
Children Act 2004	Police, local authorities (and primary care trusts) must cooperate with other relevant partners to safeguard and promote the welfare of children and ensure that arrangements are made to improve the wellbeing of children in their area.
Criminal Justice Act 2003	Clarifies the process and procedure for police and their legal basis for use.
Police and Criminal Evidence Act 1984	Provision for the secretary of state to issue codes of practice to police with statutory effects. It provides the basis for many of the police actions in respect of matters relating to safeguarding and other matters.
Children & Social Work Act 2017	Measures to improve support for looked after children and care leavers and promote the welfare and safeguarding of children. Sets out corporate parenting principles for the council.
Crime and Disorder Act 1998	Councils have a responsibility to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this.
Care Act 2014	Council's general duty to promote individual well-being and ensure the integration of health and social care and support.
Policing and Crime Act 2009	Provisions around safeguarding vulnerable groups amongst other measures

9. Appendix D: Information Sharing Checklist

The following questions must be considered when deciding whether to share information.

- Whose information is this?
- Is there a lawful basis to share the information? Justify the purpose and identify relevant legislation that applies.
- Can information be pseudonymised or anonymised ahead of sharing?
- How have individuals been informed that the information will be shared eg via a privacy notice? Will they have the expectation that their information will be shared? Consider whether notifying the individual of the sharing may place someone at risk or prejudice a police or safeguarding investigation.
- Have any requests not to share been received and considered?
- How much information is it necessary to share in this situation?
- Is the information accurate and up to date? Has the difference between fact and opinion been stated?
- Is access to the information limited to only those who need it? Is it being given to the right person?
- Is the information being shared in a secure way?
- Has the decision to share or not share, and the rationale for the decision, been recorded?