Data Sharing Agreement – Gangs Violence Matrix

Contents

1. Introduction to the Sharing

This Data Sharing Agreement [DSA] documents how the parties to this agreement, listed in Appendix A, will share personal data on MPS gangs violence matrix. 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 condition 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 that 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 Metropolitan Police Service and the London Boroughs of Camden, Hammersmith and Fulham and Lewisham. These professionals were specialists in 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, CCGs and police BCUs across London. 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 co-ordination of this agreement, but the responsibilities within it, and compliance with data protection legislation, remain with the listed data controllers.

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 platform on which this agreement is hosted (expected to be 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 or any person with access to data within their organisation. 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 the initial six months and then every year unless legislative or other changes require a more rapid review as 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 recommend 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 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.

Area of work	Description
ASB	The sharing of data regarding anti-social behaviour and related enforcement
Multi-Agency Public Protection Arrangements.	Public protection involves generally a different level of discussion to other agreements.
Prevent	The PREVENT strategy is 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	Managing the most persistent and problematic offenders through a cross-agency response to the crime and reoffending threats faced by local communities
MAS/MASH	The multi-agency safeguarding DSA covers safeguarding 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

Area of work	Description
Residual crime	A DSA to cover lower level crime not covered in other DSAs such as caution registers, nuisance, persons posing a risk to themselves, and other criminal issues.

2. Purpose and Benefits

2.1. Purpose

The Gang Violence Matrix (GVM) is an intelligence tool used to identify and risk assess gang members across London who are involved in gang violence. Everyone on the matrix has to be a gang member, and the classification as such is based on two or more pieces of intelligence. Once on the matrix, individuals are scored around violence and weapons offences, and intelligence as a victim and perpetrator. Gang members are often also victims of violence as well as being perpetrators of violence. There may be circumstances where a person assessed as low risk of committing gang violence (termed a green nominal) who is part of a gang may be on the Matrix for safeguarding purposes as a gang member who is a victim and that they may not necessarily have committed violence themselves. The matrix helps identify these victims that need support to safeguard them from further victimisation and possibly divert them away from gangs.

This Data Sharing Agreement (DSA) template formally sets out how Personal and/or Special Category Data captured in the GVM is shared Local Authorities/Council and other local partners at local level. This local DSA will interact with other core agreements, to govern how the information of those on the Gang Violence Matrix will be shared.

An investigation by the Information Commissioner's Office (ICO) in November 2018 found that the MPS use of the Gang Violence Matrix led to multiple and serious breaches of data protection laws. It issued an enforcement notice giving six months to ensure the GVM complies with data protection laws. This included ensuring that any GVM information shared with partners is done so securely and using the correct legal gateway.

The overarching aim of the matrix is to reduce gang related violence, safeguard those exploited or used by gangs, and to prevent young lives being lost. The GVM measures the harm gang nominals pose by scoring individuals on the matrix for violence and weapons offences and intelligence.

A single matrix has been introduced across London to score gang nominals so that there is equal assessment measures used to assess the risks they pose.

Matrices are owned by Basic Command Units (BCUs) who will work with and share data with their partners to enable a multi-agency approach to tackling gangs in London.

The processing is essential in order to protect the public and manage risk by working with both offenders and victims, and partnership working with criminal justice stakeholders, the voluntary and community sector. The exchange of appropriate information is fundamental to the success of any strategy implemented for the purposes of reducing re-offending and there is a sound legal basis for that sharing of information. The sharing of information also helps negate the risk around co locating rival gang members in prison.

This agreement will share appropriate information contained on the GVM with the Council in order to:

- identify offenders
- monitor them
- provide them with necessary support and assist their rehabilitation where necessary
- help them to move away from committing offences, towards a law abiding lifestyle.
- Ensure a partnership multi- agency approach to tackling gangs
- Support them by offering them opportunities including education, employment, housing where appropriate
- conduct enforcement action where required
- to safeguard gang members, their families and the community from harm

The information sharing under this agreement will allow the Council to provide the best range of services to current gang members whilst addressing any continuing offending or anti-social behaviour.

2.2. Benefits

The benefits of this DSA are to support the reduction of gang related violence by:

- taking enforcement action against the most violent gang members. This includes arrests and remand of violent gang members on the GVM
- seeking to divert and safeguard those who are victims of gang violence and/or most at risk of being drawn into gang violence by for example diverting gang members away from gang lifestyle and criminality. This will include providing them with opportunities around education, employment and training
- protecting those at risk of exploitation by gangs and the targeting of violent individuals
- support the Council's ongoing work to safeguard gang members, their families and the community, and provide gang members with necessary support and opportunities to move away from committing offences
- As less gang violence occurs, there will be an improved perception of these individuals by the general public. This will benefit young citizens, as they will not be looked on suspiciously by the general public simply because of their age
- 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.

2.3. Principles of information sharing

Effective information sharing is a vital element of the Prevention & Detection of Crime and Anti-Social Behaviour. Organisations can hold different pieces of information which need to be placed together to enable a joined up approach problem solving.

To share information, a lawful basis for doing so must be identified. This may come from legislation or from statutory guidance such as Crime & Disorder Act 1998, amongst other relevant legislation, which established the formation of statutory Crime and Disorder Reduction Partnerships (CDRP) in recognition of the idea that crime reduction cannot be the responsibility of one agency, such as the police and should be tackled by a variety of agencies working together in partnership.

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.*

2.4. 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
(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 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 Data Processing

(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)*
- *(h) Health or social care (with a basis in law) Part 2 of Schedule 1 of the DPA 2018, para 10. Preventing or detecting unlawful acts, para 11. Protecting the public and para 18. Safeguarding of children and individuals at risk*

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. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Data Protection Act 2018 Schedule 1

PART 1 Health or social care purposes

2(1) This condition is met if the processing is necessary for health or social care purposes.

(e)the provision of social care

PART 2 SUBSTANTIAL PUBLIC INTEREST CONDITIONS

Requirement for an appropriate policy document when relying on conditions in this Part.

5(1)Except as otherwise provided, a condition in this Part of this Schedule is met only if, when the processing is carried out, the controller has an appropriate policy document in place (see paragraph 39 in Part 4 of this Schedule).

(2) See also the additional safeguards in Part 4 of this Schedule.

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

10(1) This condition is met if the processing—

(a)is necessary for the purposes of the prevention or detection of an unlawful act,

(b)must be carried out without the consent of the data subject so as not to prejudice those purposes, and

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

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, probation services, 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 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.*

2.5. 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 lawful basis for some personal data processing. Each party is responsible for managing consent where they use consent as the lawful basis condition.

2.6. Proportionality and necessity

Proportionality, data minimization, necessity and not being excessive 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. It is for this reason professionals must ensure they comply with Article 5(1)(c) and share the adequate and relevant information, and limit that information to what is necessary for the achieving of the DSA aims.

There are legal safeguards which mean that it is a defence when sharing that you believed it was:

- 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
- the person acted—

  (i) for the special purposes,

  (ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

  (iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest

Professionals must record:

- the decision to share, or not to share
- the lawful basis for sharing
- to whom the information was shared

This will enable you to account for decisions made.

2.7. 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

2.8. 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 and/or for the purpose of the Prevention & Detection of Crime and Anti-Social Behaviour.

However, for the police, as a safeguard before any information is passed on, it will undergo an assessment check within relevant policies. The assessment and decision making will require the police to comply with Part 3 of the Data Protection Act, relying on section 37 to share adequate, relevant and not excessive information for the law enforcement purpose. This will allow the police to confidently share information for the protection of vulnerable persons or premises, to fulfil a legal obligation and/or legitimate interest pursued by the police. This also allows the police to share information with third parties (partner agency) when passing the information to a partner agency would facilitate a task carried out in the public interest.

Information held by other agencies that will be shared in the GVM process 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 consent has been provided or 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.

2.9. 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. Please note that any signatory organisation must consult with the MPS prior to any onward transmission of data obtained 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. Please note; any signatory to this agreement in receipt of a Right of Access request relating to a subject on the GVM should notify the MPS prior to any response being sent in order that opinion can be obtained.

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 how their data is being processed or shared will be handled under the policy and processes of 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:

- Persons on the GVM
- Relatives of persons on GVM where recorded on GVM
- Relevant professional eg social workers and police officers

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 focusses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

Information will include:

- **Personal, special category and criminal data** to enable the swift and effective safeguarding of children and improved safeguarding provision in the borough
- **Personal, special category and criminal data** for law enforcement purposes, including data defined as **sensitive data** for the competent authorities for law enforcement purposes
- **Aggregated (anonymised or pseudonymised) data** reporting to enable the partnership to further understand the safeguarding priorities.
- **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 complexity of the police and council work in these areas, 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 could be shared with the council by the police include:

- surname
- forename
- date of birth
- Ethnicity (IC) code
- PNCID (Police National Computer ID)
- name of gang they are affiliated to
- street name or nickname
- Borough Gang Violence Matrix subject is on
- BCU Gang Violence Matrix subject is on
- Matrix status (custody or live)
- non personal information concerning gang & criminal activities

- Offender RAG status (Red, Amber or Green)
- Victim RAG status

4.2. Deceased persons

It is noted that the sharing may involve data of deceased persons which 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

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,. 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.

Email is not generally a secure method of transferring personal data. Although two or more of the parties may have additional encryption that allows for an encrypted path between two of the parties, this cannot be identified simply from the email address. 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 CJSM, Egress and Encrypt and Send must be used. Description of specific transfer processes must be in relevant process documents within each organisation.

The GVM will not be shared in hard copy.

Access to the shared data will be permitted via MPS BOX (digital based storage solution) only. Access will be a preview shown on BOX. The Council is required to nominate members of staff to access the GVM in BOX and they will need to sign a user access form which explains the conditions of use.

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 suitable written agreements are in place, and that appropriate due diligence has been completed for the transfer of data. It is not intended that this data will be processed outside the UK under this DSA.

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 UKGDPR, 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 co-ordination 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.

Council users will access the GVM on Box via a web-browser, subject to access permissions controlled by the Metropolitan Police. Council users will access the GVM for reference only, and no information will be extracted or held on Council IT systems.

As no GVM data is being stored on Council hosted systems the Council will not be required to destroy or dispose of any GVM data.

5. Signatures

This agreement is signed and approved on behalf of:

The Metropolitan Police

[redacted]

Name and Rank: [redacted], Director of Intelligence

Date: 23 March 2021

Signatories will be managed through publication of this agreement onto the Information Sharing Gateway.

Version control	
Document production date	January 2021
Document currency	Draft v1

6. Appendix A – Parties to this agreement

Organisation	Duties
Metropolitan Police	• The MPS makes disclosure to third parties to fulfil the common law duties of preventing and detecting crime • statutory Law enforcement responsibilities around crime in general and gangs in particular • This will help the MPS achieve their objective of making London a safer place. • Responsibilities under legislation such as Children Act 2004 which requires the MPS to discharge its organisational functions with regards to the need to safeguard and promote the welfare of young people. • Local objectives, including the protecting those at risk of exploitation by gangs and the targeting of violent individuals will also be met.
London Borough Council	• Statutory responsibilities under safeguarding legislation to safeguard gang members, their families and the community, and provide gang members with necessary support and opportunities to move away from committing offences.
National Probation Service	• Data sharing where relevant to individuals on probation.
Others	• Other parties are expected and will be listed as signatories to this agreement when published.

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

Legislation	Main purpose of Legislation
Crime & Disorder Act 1998	This legislation established the formation of statutory Crime and Disorder Reduction Partnerships (CDRP) in recognition of the idea that crime reduction cannot be the responsibility of one agency, such as the police and should be tackled by a variety of agencies working together in partnership.
Children Act 1989 and 2004	The **Children Act 2004** is a development from the **1989 Act**. It reinforced that all people and organisations working with **children** have a responsibility to help safeguard **children** and promote their welfare

Other legislation that may be relevant when sharing information includes:

- Immigration and Asylum Act 1999
- The Localism Act 2011
- Welfare Reform Act 2012
- Common Law
- Criminal Procedure Rules 2020

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 been recorded?