PROJECT TITLE: **The Gang Violence Matrix (GVM)**

CONTACT OFFICER: Tressina Jones, London Borough of Lewisham

Explain broadly what your project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal or Committee report.
This Data Sharing Agreement (DSA) attached formally sets out how Personal and/or Special Category Data captured in the Metropolitan Police's 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. 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 must be a gang member to be included, 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. An investigation by the Information Commissioner's Office (ICO) in November 2018 found that the MPS's then 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. This DPIA and DSA are the results of work with councils and the Police to remedy the issues found by the ICO.

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows.

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.

The ISA includes statements on flows, but in general data is shared is based on need.

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.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? (guidance on intranet about what is special categories data) How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The personal data and its processing involved in these work streams 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.

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

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The benefits of this work 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.

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? Service users?

The working group approach, led by Information Governance for London group (IGfL) has been used for the Gangs Violence Matrix and is also being used for a selection of other London-wide DSAs for processes relating to crime and safeguarding duties.

This agreement is the outcome of a multi-agency working group with representation from local authorities, health and police, who have engaged with front line practitioners in their respective organisations.

Describe the lawful basis for processing the data: Which of the Article 6 and Article 9 conditions apply? Please say which are valid and what legislation allows you to operate in your service area.

Also specify which London Councils function you are working under. Consult Data Protection Officer if you are not sure how to answer this.

GDPR Article 6 (for non-sensitive data)

1. Art 6 1 (c)Legal Obligation (law says we must)
2. Art 6 1 (d) Vital Interests (life or death situation)
3. Art 6 1 (e) Public Task / Official Authority (law says we can)

GDPR Article 9 (for sensitive data - race/ethnicity, political opinions, religious beliefs, trade union membership, health/ mental health, criminal, biometric, genetic, sex life/sexual orientation)

1. Art 9 2 (c) Vital interest of data subject or another
2. Art 9 2 (g) Substantial public interest

Some of the bodies are competent bodies for law enforcement, and their legal basis is 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".*

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.

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.

Describe compliance and proportionality measures, in particular: Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

It is:

- 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.

And:

- 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

Partners will record:

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

Partners will also:

- Publish a privacy notice

Step 5: Identify and assess risks

Risk (examples listed below)	**Risk Level**	**Mitigation(s)** or note if risk is not applicable to your project	**Result:** is the risk eliminated, reduced, or accepted and what is the residual risk level?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Fair, lawful and transparent No legal basis for the processing, processing may not be necessary or proportionate. The processing is without a Privacy Notice.	Medium/high	Legal basis has been identified in the DPIA and DSA. DPIA will be reviewed in the first 6 months then annually thereafter which will allow proportionality to be reassessed. Privacy notice to be provided on websites, and considered there is an exemption to need to provide to individuals when GVM accessed. This risk relates to the GVM itself which is a risk handled by the police. Councils' access to the GVM is lower	Risks reduced/eliminated, residual risk Low	Yes

The processing is inherently privacy intrusive, labelling individuals as gang members and sharing that with 3rd parties.	High	risk being access of fewer people, and as much councils' work on this area will be to the benefit of those on the GVM the intrusion is lessened.	Reduced, residual risk medium	Yes
Purpose Purpose creep: data used for something it wasn't collected for, a breach of purpose limitation.	Medium	Access is by a small number of individuals working in the area who will be trained and have clear parameters for access and usage. DPIA will be reviewed in the first 6 months then annually thereafter.	Risks Reduced, residual risk Low	Yes
Data Minimisation Too much data collected that's not necessary	Medium	Data is collected by police and not councils who access the police's data. This risk is therefore owned by the police. DPIA will be reviewed in the first 6 months then annually thereafter.	Eliminated, residual risk low	yes

Data accuracy Inaccurate data collected, Data corrupted or metadata altered by users. Users forget they have shared files or Files shared/deleted incorrectly	Medium	The Data is collected by police and not councils who access the police's data. This risk is therefore owned by the police. Not data can be downloaded by councils who have read only access.	Risk owned by police, eliminated, residual risk low	Yes
Retention and disposal Data kept for too long, No records of destruction kept.	Low	Councils have read only access to BOX and cannot download data. Any data recorded eg nomnal status in council records will be subject to council retention periods. 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. All partners must a destruction of records policy in place. Information must not be retained for longer than necessary for the purpose for which it	Low	Yes

		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.		
Security Inadequate security around access and control of the system leading to unauthorised access and use of data, malware concerns and security and physical breaches. Caused by any one of: Access controls not in place, Monitoring and audit controls not in place, malware controls, patching, virus protection etc. not in place, Authentication not strong enough, Poor physical or technical security,	Medium/high	Access to MPS BOX will be limited, recorded and user will sign a user access form which explains the conditions of use. Access to council systems are monitored. The council operates a patching process and deploys malware and virus protection and has appropriate technical security measures including a password policy setting out requirements in line with best practice. Council have appropriate physical security measures in place. Access to BOX is by named trained officers, so there is full RBAC in place. Access to MPS BOX will be recorded and users will sign a user access form	Reduced or eliminated, residual risk is low	yes

Unpermitted access by third party / employee, Staff not adequately trained, theft of data.		which explains the conditions of use. Information will not be sent from BOX.		
Data subject rights Data subject requests are not responded to in required timescales.	Low	The met is the data controller for the GVM and responsible for handling data subject request relating to it. Councils will handle requests relating to information they hold in accordance with their existing policies and procedures.	Reduced residual risk low	yes
Transfer outside UK Data transferred or stored outside UK e.g. in cloud without adequate safeguards. Backups held outside UK, without adequate safeguards. Staff users send personal data insecurely outside UK due to lack of physical controls in place.	Low	All Data is held within the UK and there would be no reason for councils to send data out of the UK. Where external transfers are made councils have processes in place to ensure all UK GDPR requirements are met	Eliminated, residual risk Low	Yes

Overall risk rating for project: medium

Item	Name/date	Notes
Measures approved by:	Each party to the agreement	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Tressina Jones	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Each party must ensure that its DPO reviews this DPIA, and documents any agency-specifics necessary. Camden's DPO Andrew Maughan the Borough Solicitor has reviewed the DSA and advised:		

I am happy with the approach here and that this processing with the mitigations listed is lawful and appropriate