London Gang Exit

Data Protection Impact Assessment

Delivered by:

saferlondon

Commissioned by

MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

November 2019

Document information

Master location	:	[redacted]
File name	:	LGE_DPIA_DraftV3
Distribution	:	MOPAC and LGE delivery partners only
Author(s)	:	MOPAC / SAFER LONDON

Version control

Version no.	Version date	Summary of change	Author
V1	May 2018		[redacted]
V4	Jan 2019		
V10	Apr 2019		[redacted]
V13	Sept 2019		[redacted]
V14	Nov 2019		[redacted]
V15	Nov 2019		[redacted]

1. GENERAL

1.1 Introduction

This Data Protection Impact Assessment (DPIA) outlines the data processing which will be conducted by the Mayor's Office for Policing And Crime (MOPAC) in-house research team, namely Evidence and Insight (E&I) unit, for the purpose of the London Gang Exit (LGE) evaluation. This document details the lawful basis used to access and process data and conduct research; provides an understanding of responsibilities, risk and mitigation; lines of accountability; and aims to provide reassurance and transparency to members of staff; clients who access London Gang Exit; members of the public; and our elected officials.

London Gang Exit (LGE) is a pan-London multi-agency intervention, originally jointly commissioned by the Mayor's Office for Policing And Crime (MOPAC) and the London Community Rehabilitation Company (CRC). LGE commenced in February 2016 and was initially funded until October 2017. MOPAC took over sole funding of the project after this date and LGE is currently funded to March 2020. The programme is being delivered by a consortia led by Safer London, and including Catch-22/Only connect. Redthread ceased to be a delivery partner in April 2018 but continue to work alongside Safer London as an embedded referral partner. The pan-London service was designed to complement and enhance existing local services, filling gaps in provision of support services for young Londoners who are involved or affected by group violence. MOPAC's Evidence & Insight Team (E&I), the evaluation seeks to explore the process of implementation as well as any impact of the intervention.

The London Gang Exit evaluation will focus on four distinct areas for analysis, building in complexity. These are performance review; process evaluation; impact evaluation with an aspiration to economic evaluation. The ability to successfully complete each element will depend on data quality and quantity and will be reviewed throughout the life of the research.

The performance review will utilise data and management information captured during the everyday running of the London Gang Exit. Case data is captured and managed on Safer London's Lamplight Case Management System (CMS). Data will be provided to MOPAC for oversight of contract management and for the purposes of the evaluation (please see Section 2.1.3 Data Storage and Transfer for more details). Performance data used for the evaluation will monitor aspects such as (but not limited to), how many clients are using the service and when; what needs they present with; what services they receive and for how long.

The process evaluation examines how the initiative has been implemented and includes gathering feedback from all those involved (stakeholders; staff; and where possible service users and families) to identify key learning and good practice, as well as challenges and suggestions for improvement. Methods are largely qualitative (interviews and / or focus groups) to better understand the implementation process, partnership-working and integration of services, but importantly the experiences of those delivering, as well as those engaged with the service.

The impact evaluation aims to examine if London Gang Exit has delivered its desired outcomes and how it has affected those who are involved. In order to robustly evaluate impact and work out which key aspects or 'ingredients' of the service provided by the London Gang Exit intervention have an effect, E&I aim to identify a counterfactual or control group (i.e. a matched group who do not receive the London Gang Exit intervention) against which to compare the outcomes and experiences of those who do receive the London Gang Exit services. This data will come from a variety of sources including

CRIS and the Matrix; but also CRC/NPS (of which data sharing agreements have been produced). Outcomes can then be compared for both groups before and after the intervention (i.e. LGE) is put in place. Robust matching at the cohort or individual level is planned to ensure the validity of the counterfactual being used.

Finally, cost data relating to the set up and running of the London Gang Exit will be captured to conduct an economic evaluation. This information will be balanced against key literature exploring the benefits (to the individual or to wider society) from such programmes and be able to answer questions such as 'Does LGE provide value for money?' and 'What are the public value benefits and what are the fiscal benefits?'.

This document outlines the data processing activity conducted by the MOPAC for the London Gang Exit programme, primarily concerning data management, risks and mitigation for MOPAC contract management and the E&I led evaluation. It should be read in conjunction with Safer London's information governance documentation (Safer London Information Sharing Policy v. August 2018). It will identify where personal and/or special category or criminal offence data is being used and describe the arrangements for how data will be processed.

This project requires a DPIA because it involves the processing of Personally Identifiable Information (PII), in particular that of potentially vulnerable children and young adults, who have been victims and MOPAC delivers them for best practice and to ensure we have documented our thinking when delivering research. In addition to PII MOPAC E&I will also be processing special category data, potentially:

- race
- ethnic origin
- health (including mental health)

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. To lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These are outlined in this DPIA (see Section 4.1.1 Legal) and describe which data is gathered under which basis e.g. consent for LGE records and public task for MPS data.

MOPAC E&I will also be processing criminal offence data, in its official oversight capacity (see Section 4. Legal). To process PII about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. These are outlined in this DPIA (see Section 4.1.3 Legal).

This DPIA is intended as a 'live' document which will be updated regularly, and this and relevant Safer London data governance documents will be reviewed, at a minimum, annually.

2. Data Processing

2.1 The nature of processing

This section documents how data will be collected and processed for the purposes of the London Gang Exit evaluation. Personally identifiable information (PII) collected and analysed will only be that which is necessary to meet the requirements set out in this agreement. Data will only be processed for the purposes for which it was obtained and for other purposes which are not incompatible - such as (and only where justified) research and analytics. Wherever possible data minimisation principles will be applied and PII will be de-personalised at the earliest opportunity. Whilst this DPIA concludes a

significant amount of personal and sensitive data will be processed, safeguards are in place to ensure compliance with Data Protection principles and the risk assessment outlines details associated with the project and the proposed mitigation (see Section 6. Risk Assessment). The lawful basis for obtaining and sharing data is outlined in Section 4.

In the main, data is classified as OFFICIAL SENSITIVE under the Government Security Classification (GSC). Data is personally identifiable (e.g. information relating to a living identified or identifiable individual, including name, address, dob, id number, location data, online identifier or one or more factors specific to someone's physical, physiological, genetic, economic, cultural or social identity) and in many circumstances is special category (e.g. data relating to racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences) making it open to additional security measures or appropriate safeguards (see below for more details). Criminal offence data will be processed – this data includes information about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act. However, under the GDPR the category is potentially broader, with Article 10 specifically extending to personal data linked to related security measures. To process PII about criminal convictions or offences the processor must be under the control of an official authority; or when permitted under EU or Member State law (see Section 4. Legal for more details).

2.1.1 – Data Source & Collection

This project has three main sources for E&I data each with their own methods of data collection:

1. London Gang Exit case management system (Lamplight CMS)
2. Metropolitan Police (MPS) data
3. Bespoke evaluation data – primary data collection

Access to personally identifiable information (PII) will be restricted, even within E&I on a need to know basis (see Section 2.1.3 Storage & Transfer). See Section 6. Annex A – Data sources and transfer.

London Gang Exit case management system (Lamplight CMS)

The CMS is owned by SL, but combines data recorded by staff employed by several organisations (namely Safer London, Only Connect/Catch-22, Rethread, National Probation Service, London Community Rehabilitation Company and the MPS), the majority of which has been specifically collected as a new record for the London Gang Exit programme. Data is PII and will include, but not be limited to: client demographics; health, social care, mental health, and information regarding their interventions. SL has overarching documentation outlining how organisational data will be collected, used and stored in the CMS and how data minimisation techniques will be employed, to limit access for the different partners (and roles) to only essential data (see Safer London Data Protection Policy v. November 2018). Whilst the evaluation requires a wide breadth of data, E&I employ the same data minimisation principles and do not require access to everything on the CMS - the agreed fields will be added at a later date, closer to extraction – (Section 6; Annex B provides examples of thematic data to be collected).

Metropolitan Police (MPS) data

Criminal justice data will be required for the evaluation. Most of this will be obtained from the MPS, utilising the existing relationship between MOPAC and the MPS to obtain a relevant sample. This relationship is further described in the Information Sharing Agreement (ISA) (Ref: MOPAC/MPS/2018/01) and relies upon MOPAC's lawful basis of public task, under its core oversight

function stipulated in the Police Reform and Social Responsibility Act 2011. The PII will be drawn either by E&I staff directly from the MPS Crime Recording Investigation System (CRIS) or by MPS staff from the Police National Computer (PNC). The acquisition of PNC data is currently being addressed as part of MOPAC's overarching Information Sharing Agreement with the MPS (see Section 6: Risk Assessment). The MPS data will be used to monitor police contact, victimisation and offending. For the final evaluation report, impact on criminal behaviours will be measured through proven reoffending. There is a potential that a counterfactual may draw on data from within the MPS systems.

As detailed in the ISA (Ref: MOPAC/MPS/2018/01), E&I staff will follow standard practice and access MPS data directly via the MPS information technology terminals (FOUNDATION). Staff are therefore held to account via the same policies and procedures as the MPS when accessing and processing data via the FOUNDATION architecture. This also includes, but not limited to, Management of Police Information (MOPI) and Computer Misuse Act. E&I staff are trained on each system and act as 'readers' or 'reviewers' – they will not be permitted to make changes to the information inputted by the authors (the MPS). Where errors are identified staff will follow the procedures set out in Section 4.5.

Bespoke evaluation data – primary data collection
Across the course of the evaluation bespoke information will be gathered through primary data collection techniques (such as interviews and focus groups), by E&I. Where possible, data will be anonymised and therefore not PII. This includes the potential for qualitative analysis of case notes – where valuable context about providing the service can be gathered, but without identifying the individual involved. Participants may include, but not be limited to: Gang Exit service users; London Gang Exit Staff; stakeholders; and wider professionals. Bespoke data collection involves the collation of cost data. In these cases, despite information not being PII, permission for participation will be sought (see Section 4. for legal basis) to fulfil an ethical and transparency requirement. If there is a need to collect PII for bespoke evaluation data, this will be done under the strict consent parameters and this DPIA will be updated accordingly.

2.1.2 – Use of data
As highlighted in the 'Introduction', data is required for potentially four stages of an evaluation - the performance review; process evaluation; impact evaluation and an economic evaluation. Each stage will enable stakeholders to monitor the programme's progress and/or impact effectively. Most of the data will be collected by Safer London, the owner of the CMS. Data follows an individual's progress through the intervention, from initial referral to completion or removal from the programme (see Annex A). This data will be collected from multiple sources (i.e. caseworker notes, client feedback, harm/risk/need data from partners and third-party organisations) and collated on the secure Safer London case management system, Lamplight.

MOPAC will only be provided with a sub-set of this data, to employ data minimisation principles, at specific points in the programme's life. For this data MOPAC will act as a controller for the data it receives from SL (see Section 4. Legal). This data will inform Payment By Results (PBR) analysis, interim evaluation reports and the final evaluation report. MOPAC will supplement data with that from MPS/Police databases (PNC, CRIS, Gangs Matrix) to inform the evaluation – although data will not be shared with the MPS or back with SL (see Section 2.1.6 Data Sharing).

Data is required to enable MOPAC E&I to monitor the programme's progress and impact effectively. For the purposes of the programme data will be gathered and processed which is required to:

- Identify individuals taking part in the intervention programme, as well as those who have been accepted but did not complete for any reason.
- Monitor progress across intervention strands, as well as client and caseworker perceptions of progress.
- Assessing the risk and need a service user presents with; how this is matched to the intervention provided by SL; and how these may change over the course of the evaluation.
- Understand previous and future involvement in criminal activity and violent victimisation to assess the impact of the intervention.
- Assist in the evaluation informing future policy formation and implementation.
- Data from programme staff by way of surveys and interviews as part of the process evaluation.

Information used by MOPAC will be reported at the aggregate, not an individual level and not used in a way whereby an individual can be identified by any means (e.g. reporting on data with small base sizes). This includes location and mapping data; survey or interview answers; crime and victim data; and staff information (e.g. HR records). Reporting may take the form, but not be limited to: internal written documents or briefings; data visualisation packs or dashboards; info-graphics; journal articles or published documents; and may include case studies or quotes from research participants.

2.1.3 – Data storage and transfer

The majority of London Gang Exit will be recorded on the bespoke Safer London Lamplight database (CMS) (See Safer London Information Sharing Policy v. Aug 2018; Data Protection Policy v. Nov 2018; Data retention archiving and deletion v. 1b November 2018). Data from the CMS which is required for the evaluation (see Annex B) will be provided to MOPAC E&I unit. This transfer of protectively marked information up to the level of OFFICIAL will be done electronically using secure email. (Please note, pnn, .gsi, .cjsm, Egress and nhs.net are examples of secure email, .gov.uk and nhs.uk are not secure). All MOPAC employees have both MPS email addresses (.pnn) and MOPAC addresses (.gov.uk). Whilst the (.gov.uk) address is now fully encrypted - Forcepoint is in place meaning all MOPAC's outgoing emails are encrypted to the government recommended standard of TLS 1.2 (Transport Layer Security (TLS) Protocol. This protocol is an industry standard designed to protect the privacy of information communicated over the Internet) – for the purposes of information transfer for London Gang Exit only the (.pnn) address will be used (as per the ISA Ref: MOPAC/MPS/2018/01). The file will be password protected (or sent in an equivalent locked format) and details of the password will be sent separately to the data.

On receipt of the CMS report; for data primarily extracted from the MPS Systems; and for data gathered for the evaluation (e.g. interview transcripts etc), information will all be stored electronically on the MPS FOUNDATION architecture as per ISA Ref: MOPAC/MPS/2018/01). The location of PII will be (e.g. the file path) will be recorded on the MOPAC organisational asset register.

Staff that will access the data will have been vetted to the relevant level. MOPAC E&I staff are security cleared to at least Counter Terrorist (CT) level. Usually MPS data stored in FOUNDATION will be retained in the original system used by the authors of the data (MPS). There are occasions where this is not the case (E.g. storing CRIS or PNC output in an EXCEL format so crime analysis can occur). In these circumstances MOPAC E&I will store data in their own area of FOUNDATION Shared Drive and apply the retention polices set out in this document (see Section 2.1.4 Data Retention). Access to E&I's FOUNDATION folders are limited to named E&I staff and PII will be further restricted, even within E&I, on a need to know basis. This is achieved by limiting folder access and applying passwords to spread sheets. It has been confirmed that access to the information can be audited.

When online surveys are used to collect data from stakeholders and staff members, an online portal will be used to create the survey and record the responses. The online portal is run by a company contracted by MOPAC/MPS called Opinion Research Services (ORS). They have their own specific documentation for which the storage of these responses must adhere (Contract Ref: SS31380). Where possible survey information will be non-PII, but permission will still be sought to participate (see Legal Section 4).

If any other external companies are used as a processor during the evaluation (e.g. to conduct client interviews), this element of the research will require additional bespoke documentation to outline the agreed processes by which a company must adhere and this DPIA will be updated accordingly.

Where papers are used, MOPAC employs a clear desk policy. Anything of an OFFICAL marking will be stored in a locked container within a secure premise with a managed access control. Access to information will be limited to those with a genuine "need-to-know". When the documents are not being used they will be locked away.

There should be no need to back up electronically held information via disc, hard drive, or any mobile device, but if this is deemed necessary then the appropriate level of encryption and or password requirements must be in place. This should be followed by the media used being stored in a physical location that has a level of security appropriate to the level the information held is graded to. The relevant security standards set out by the GSC for transmitting, storing and disposing information must always be adhered to. Likewise if information is to be stored on removable media, these will be encrypted to government standards and passwords will be in place. Only an encrypted MPS approved Datashur USB must be used (available on PSOP), as CDs are no longer acceptable.

For focus groups and/or interviews non-PII of stakeholders/staff is sometimes stored for a short time as voice recordings on Dictaphones. This information is removed from the mobile device onto the MPS FOUNDATION system at the earliest opportunity.

There should be no need to physically exchange information under this agreement. However, should the need arise, exchange will take place by a trusted person in a closed container or package. Subsequent movement within MOPAC must be treated with the same degree of security. Information moved by post or courier will be done in a sealed package with no protective markings showing (other than PERSONAL or PRIVATE). It will be addressed to a specified individual within the partner organisation by name or appointment (add job title).

Speech will be guarded and conversations will be kept short when sharing information via telephone and the use of fax will be avoided for transferring protectively marked information as it is not secure.

2.1.4 – Retention and Disposal

All parties carrying out the functions set out in this agreement must adhere to their organisation's record management policies and procedures specifically in relation to retention and destruction of data. Such policies and procedures must be GDPR compliant. For the CMS and all organisations involved in London Gang Exit, the overarching documentation (Ref: Safer London Data Retention, Archiving & Deletion v. November 2018) will outline the disposal procedure.

MOPAC have documented their retention criteria in MOPAC'S Information Governance policy, where public consultation research falls under a retention period of 8 years. For E&I data the general rule is 'all files containing MPS, PII or sensitive data will be assessed on conclusion of the project and deleted'. Where there are exceptions (for example in some instances data may be required for historic or longitudinal research purposes), these will be detailed at that time in the DPIA; only the minimum

amount of data is retained; and its whereabouts will be recorded on the organisation asset register. If data can be made non-PII it will be done as soon as possible. If the deletion of personal data is for some reason not possible, it will be placed beyond use with limited access.

Hard copies of information will be destroyed when it is no longer of relevance under the agreement. Papers will be disposed of through an OFFICIAL SENSITIVE waste system - either via the confidential waste disposal system, or via a cross-shredder; and where possible on MPS premises. Electronic information will be securely erased or overwritten using an approved software utility to a standard applicable to the protective marking.

2.1.5 – Correcting erroneous data

If during an individual reviewing their own data under the 'rights to access', or in the course of E&I staff processing data it is found something is incorrect, MOPAC will contact the data authors (the MPS or Safer London) to rectify information.

Where the MPS are authors MOPAC will contact the MPS via the Information Assurance Unit). Where Safer London are the authors, MOPAC when acting as a joint controller of CMS data (for the purpose of conducting the evaluation), contact will be made via the service manager at London Gang Exit. The owning organisation may not be able to change the information unless it is found to be an input error. Any dispute regarding the accuracy of the data or continued refute to the validity of information will be noted. Further details of these processes can be found in the overarching SL documentation (Ref: Safer London Data Protection Policy v. Nov 2018; Safer London Data retention archiving and deletion v. 1b November 2018).

All staff have a duty of confidentiality and a personal responsibility to safeguard any information with which they are entrusted. This includes ensuring that they comply with the legal and regulatory requirements and standards, for example the encryption of personal data on removable media.

2.1.6 Data Sharing

The following groups have access to some or all of the project's data:

- **Safer London**, as CMS owner and Data Controller. Safer London will not have access to individual level police data gathered by MOPAC E&I. That provided to them by the MPS will be covered under their own data sharing agreements (Ref: A purpose specific DSA between MPS and Safer London delivering London Gang Exit).
- **MOPAC,** as Data Controller will be given data generated from the CMS. To employ data minimisation principles, MOPAC will not routinely access the Lamplight database containing the personal information, needs and ongoing assessment of individuals. However, as commissioners and evaluators of the pilot service, they will be recipient (via secure email) of a sub-set of records and reports from Safer London. MOPAC will not share police records extracted. MOPAC has no onward flow of individual level data; anything disseminated from MOPAC will be anonymised or aggregated in accordance with GDPR.

It is understood that MPS information obtained for policing purposes, will not be used in any manner contradictory with those purposes. MOPAC policy is to not share PII derived from MPS sources with other agencies, providers or third parties. This means once the CMS extract is obtained from Safer London and merged with MPS data for criminal justice analysis, this PII will not be shared back with any of the organisations involved in London Gang Exit. Anonymised and aggregate data in the form of performance information or reports can be shared. If there is a requirement to share MPS sourced PII,

this process will need to be captured in bespoke ISA/DPIAs. Any decision not to share certain information should similarly be recorded along with the reasons for the decision.

When MOPAC uses MPS information in conjunction with data from other sources, there is also an overarching understanding that PII will not be shared back with the MPS. This means that any data from the SL CMS will not be shared with the MPS. If it is felt there is an acute need to share MOPAC E&I held data with the MPS to make policing decisions, agreement will be sought at that time from the lead provider, and where possible this data should be transferred by SL, not MOPAC E&I.

There may be exceptions to sharing PII with an external agency for bespoke commissioned research, where they are acting as MOPACs processor - such as interviews with vulnerable clients or family members. Contractors may become aware of names or case details and will therefore be required to adhere to bespoke processes. Where this occurs MOPAC E&I will complete a bespoke ISA/DPIA to stipulate the role of the Data Processor. This will be in partnership with Safer London to ensure all risks are considered and mitigated. This will include, but not be limited to, the need for the contractor to pass the relevant vetting level (RV and CTC); demonstrate data can be stored securely; confirm they will adhere to the stipulated retention/deletion guidelines; and confirm data will not be shared data with any other parties.

Should stakeholders require access to data for other reasons or other data held by MOPAC E&I, they will need to submit an External Agency Request (EAR) to the MOPAC project manager, Ashley Herron via secure email. The request must explain why access to the information is required and failure to provide sufficient justification will lead to it being rejected. Information will only be released in accordance with the provisions of GDPR unless otherwise directed by a Court. This will be the minimum amount of data necessary to comply with a valid EAR and where possible, it will be binary data (e.g. received therapeutic services – yes/no). Any release of data will be done in partnership with the original data owners (SL or the MPS) and where possible will be transferred by them.

2.1 THE SCOPE OF THE PROCESSING

The data E&I utilise, including that from the CMS and MPS systems, generates legitimate concerns about data privacy and the management of personal information, especially considering the sensitive nature of the victim information recorded and potential vulnerabilities of the individuals involved. MOPAC E&I will ensure procedures outlined in the DPIA and the referenced Safer London data governance documents will be followed to reduce the risk to the LGE partners, the public, the MPS and MOPAC.

2.2.1 What types of data and geographic area

The PII E&I will process as part of the LGE evaluation will in the main relate to vulnerable young people who have been victims or perpetrators of gang related violence or exploitation (see 2.2.2 special category and criminal offence). Data may also include limited details of family members.

To be eligible for referral to London Gang Exit the individual (male or female) is required:

- To be aged between 16-24 who are affiliated with or involved in gangs.
- To be at significant risk of harm from gang activity, (such as through child sexual exploitation), or a risk to themselves, or posing a risk of harm to others.
- To show some motivation to end their gang involvement and a willingness to cooperate with the LGE service.

The young person will not be eligible:

- If they are not yet motivated to end their gang involvement.

- If they are already receiving extensive support from the borough that they are residing in, or from other statutory organisations, or if the services they require are already available locally to them.
- If they fall outside the eligible age range.

LGE is a pan-London initiative; clients are taken on from all London boroughs (at the time of writing referrals have been accepted from all but one).

Data will also be collected from staff and stakeholders who have had, or are currently involved in LGE implementation and/or delivery; and those who may be referring clients to LGE. These are likely to include, although not limited to, commissioners, lead provider, LGE staff members, service providers for the intervention strands.

2.2.2 *Does this include special category and/or criminal offence data?*

This project involves the processing of PII, of potentially young adults, who may have been victims of violent crime. In addition to PII MOPAC E&I will also be processing special category data, potentially:

- race
- ethnic origin
- health (including mental health)

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These are outlined in this DPIA (see Legal section 4.).

MOPAC E&I will also be processing criminal offence data, in its official oversight capacity (see Legal 4.). To process PII about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. These are outlined in this DPIA (see Legal section 4.). The criminal offense data obtained from CRIS/PNC will be analysed to understand the offence and the progression of the case through the criminal justice system.

2.2.3 Volume of those affected (How much & how often)

Based on throughput figures to date, it is estimated that approximately 200 will have completed the LGE programme by the time of the final evaluation report in Autumn 2019. Safer London estimate that overall around 520 will have been worked with to some extent by this over the course of the pilot (i.e. some level of detail will be inputted on CMS). It is anticipated that all cases will be inputted into the CMS and potentially in scope to be included in the research. This figure may be affected by Various implementation issues including resourcing and/or funding extensions.

The number of cases used for analysis from the CMS will be matched to CRIS and data extracted to allow for offending and victimisation analysis. There exists and an element of flexibility based on resourcing levels and it is more likely to be conducted after 12 or 18 months of data collection, to allow cases to progress further along the CJS and for a bigger sample size. The methodology and hence sample size and for identification of the comparison group is to be decided.

It is expected that any qualitative analysis such as interviews with clients; anonymised case studies; staff focus groups or interviews will be with less than 20 people. The volume of stakeholders and staff members involved in surveys for the evaluation will fluctuate dependent on recruitment, but it is estimated to be fewer than 40 people per survey. Surveys are expected to occur at 4 main points

throughout the evaluation life cycle; interviews will be less frequent. Interviews or feedback from clients will only occur at twice (interim report 2 and final report).

2.2 The Context of Processing

MOPAC has different roles to play with regards to data depending on the specific part of the evaluation. For example, Lamplight data sent by Safer London falls under their role as a controller with Safer London and partners. Access to MPS data by MOPAC for the purposes of evaluation is to follow the pre-agreed process whereby a proforma is completed by MOPAC and signed off by both MOPAC and the MPS. The terms of agreement will include MOPAC plans for storage, anonymization, retention and disposal, and management of risk regarding the processing of this data. Only specific/seconded individuals from MOPAC E&I are able to extract and work with the data (i.e. run the query, quality check and anonymise data). Risk and mitigation for each part of the evaluation has and will continue to be assessed and recorded in the relevant DPIAs, but MOPAC will follow overarching principles to inform individuals of their data rights to ensure all work is compliant with the GDPR.

2.3.1 Relationship with Subjects and Transparency

Every effort will be made to be as transparent as possible. MOPAC publicises its privacy notice and how it uses data on the public website[1]. It is unlikely that members of the public would understand that their data is used for research and analytical purposes. That is why MOPAC mainly, and where appropriate, relies on its lawful basis of public task, as it has a clear mandate in law, and has been advised to use in this way by the ICO (see Section 4.1 Legal).

This includes details of transparency, such as how information will be provided to individuals (using age appropriate language and detailing the ways in which their data will be used); the Fair Processing Notice; how individuals can obtain information on their privacy rights; and submit Freedom of Information request or subject access requests. Please refer to Safer London Data Protection Policy v. Nov 2018 – Fair Processing.

A review of the transparency process as part of the ongoing development on this DPIA highlighted a specific issue relating to the naming of MOPAC as a commissioner in the Privacy notice for service users.

- *Active service users* – are those who have signed up to LGE and have seen the post GDPR privacy notice (see appendix one). There is considered to be a transparency issue as MOPAC are not specifically named as commissioners of the service, accessing PII. As with 'Future service users' there needs to be a process to inform people MOPAC will be conducting service evaluation. Following ICO previous advice, MOPAC are still being provided PII under the public task justification, therefore not offering the strict ICO 'consent' parameters. However, although service users will not be explicitly opting in, MOPAC E&I are prepared to honour an 'opt out' if they specifically do not want their PII to be used *and* contact accordingly. It is suggested this is offered via email to existing service users, but as the evaluation relies on obtaining enough data to use, SL staff may need to do some prior engagement with service users to elevate any concerns/answer any questions (e.g. FAQs and data flow).

[1] https://www.london.gov.uk/about-us/governance-and-spending/privacy-policies/mopac-privacy-notice

Detailed in full in a briefing note to Safer London (April 1st 2019) and the matter is currently being addressed with a recommendation that the privacy notice is amended to explicitly state MOPAC is key commissioner of LGE and active clients be updated with this information accordingly.

MOPAC will be conducting its research on the basis that it aligns with the original purposes for which it was collected, or a purpose that is not incompatible with that aim.

For other potential PII processed as part of the LGE Evaluation (such as via interviews or focus groups), either permission from professionals or consent will also be sought – although most of primary collected data will be non PII in nature.

2.3.2 How much control will the data subjects have?

All LGE PPI data will be processed under Section 143 of the Anti-Social Behaviour, Crime and Policing Act 2014. Clients are free to submit Subject Access Requests via the authors of the data (e.g. the MPS, or SL), to view the data held on them (see Subject Access Requests and Safer London Individual rights to access information v. October 2018). Clients can access details as to how their information is used via the Metropolitan Police Service's website[2].

2.3.3 Would they expect you to use their data in this way? How are you ensuring the unexpected doesn't happen for the subject? How are you ensuring transparency?

Upon admittance to the programme, clients are advised the data collected on them will be used for evaluation purposes. Likewise, staff and professionals will be given a full explanation when collecting data via interviews, focus groups, surveys etc.

2.3.4 Do the data subjects include children or other vulnerable groups?

London Gang Exit has service users aged under 18, and includes vulnerable groups. Under the GDPR children need particular protection when collecting and processing personal data because they may be less aware of the risks involved. Thought has been given and documented in SL overarching documentation to protect them from the outset, and to design systems and processes with this in mind. (i.e. SL have developed an accessible age appropriate privacy notice and information and actively ensure that they have understood this, its possible ramifications and are happy to work with us with this in mind, explicitly stating that service users have had the opportunity to ask any questions they may have.)

2.3.5 Are there prior concerns over this type of processing or known security flaws?

MOPAC E&I process PII, special category and criminal offence data as part of their everyday role. Any breaches of data protection or policy follow the breach procedure and are logged internally for future learning (see MOPAC's Data breach process and the overarching Safer London Data Breach Policy and Guidance v. September 2018). In the 4 years E&I has been operating, in its current form, there have been no notifiable data breaches required to be reported to the Information Commissioners Office (ICO). MOPAC have engaged with the ICO to specifically discuss the Child House project and mitigate any risks.

In the 2 years SL have been using lamplight and delivering LGE there have been no ICO notifiable breaches of PII.

2.3.6 Is it novel in any way?

[2] https://www.met.police.uk/rqo/request/

London Gang Exit is of itself a unique programme in London. However, the concept of bespoke support for individuals involved in gang related criminality has been employed in similar forms both in London and across the world. The relationship between delivery/commissioning partners – in particular the inclusion of so many data controllers is novel. All details about its risk and mitigation are included in this DPIA (see Section 6. Risk Assessment). There are no new or novel techniques being employed for the evaluation.

2.3.7 What is the current state of technology on this area?

Any novel use of technology will incur additional risk and should be documented, as it brings with it unique circumstances regarding the access; storage; sharing; and retention of data – especially at the end of the programme. Lamplight, the CMS used by Safer London is an established software package for charities used by over 400 organisations. The Lamplight data-centre is accredited to ISO27001, among others – details of compliance with numerous security and Information Governance standards is available at https://aws.amazon.com/compliance/. (See also http://www.lamplightdb.co.uk/the-system/gdpr/). See also: Safer London Data Protection Policy v. Nov 2018; Safer London Data retention archiving and deletion v. 1b November 2018; Safer London Information Sharing Policy v. Aug 2018

2.3.8 Are there any current issues of public concern that you should factor in?

We recognise that GDPR is new and still evolving and none of this has been tested in law, although is at the forefront of current public debate. We will continue to use the DPIA as a living document to identify and minimise risk.

The handling and use of police data to confirm or identify gang affiliations or connections is a controversial and sensitive topic. This includes significant concern from communities, academics and human rights organisations around police data sharing in relation to this (see https://www.london.gov.uk/mopac-publications-0/review-mps-gangs-matrix).

Learning from the MOPAC E&I Matrix Review has highlighted the particular concerns and risks around identification, collation and sharing of lists which identify individuals as gang members. It is important to reiterate that the data collected by Safer London and analysed by MOPAC E&I as part of the evaluation is not shared with or accessible to the MPS at an individual (i.e. PII) level.

2.3.9 Are there any approved codes of conduct or certification schemes that you can sign up to? (once approved)

MOPAC E&I will undertake the following actions to ensure they are conducting rigorous and ethical research (see consultation section). This includes but is not limited to: presenting research plans to the programme board and external, interested stakeholders; ensuring the lead provider is sighted on plans.

2.3 The Purpose of Processing

MOPAC's E&I unit processes a vast amount of PII and other data as part of exercising statutory and other duties in relation to the Police Reform and Social Responsibility Act 2011 and the Mayor's vision of a 'Safer City for all Londoners', as per the Police & Crime Plan 2017- 2021[3]. Whenever a project or specific programme of work is being undertaken, MOPAC and associated partners produce a specific DPIA outlining risk and impact for those specific circumstances. This evaluation DPIA for the London Gang Exit programme outlines the specific purpose for processing PII. PII collected and analysed will be only that which is necessary to meet the requirements set out in this document. Data will only be processed for the purposes for which it was obtained and for other purposes which are not

[3] https://www.london.gov.uk/sites/default/files/mopac_police_and_crime_plan_2017-2021.pdf

incompatible, such as (and only where justified) research and analytics or the prevention or detection of crime and be deleted as soon as possible.

2.3.1 What do you want to achieve?

- assess if the programme has met its aims and therefore been a 'success'. LGE aims to:

	Outcome	**Measurement**
	Outcome 1: Reducing / ceasing involvement in gangs	Of the young people starting on the programme involved in gangs there is a reduction in involvement or ceased involvement at the end of the programme
	Outcome 2: Reduction in harm caused by gang-related activity	Of the young people starting on the programme experiencing gang related harm, there is a reduction in harm at the end of the programme
		Victimization. Reduction in reports of victimization comparing 6 months before the programme and 6 months from the start of the intervention.
		Severity of offending. Reduction in severity of offences (violence to non-violence; drug dealing to drug using etc.) comparing 6 months before the programme and 6 months from the start of the intervention.
		Time taken to reoffend. Increased amount of time between offences comparing 6 months before the programme and 6 months after the start of the intervention.
		Frequency of offending. Fewer arrests / charges comparing 6 months before the programme and 6 months after the start of the intervention.
	Outcome 3 : Improved access to pathways of support	Of those identified as needing housing and money management support, there is an increase in the number either accessing and/or increasing their ability to access housing by the end of the programme
		Improving health and well-being: Of those with an emotional or physical health need, there is an increase in the number reporting an improvement by the end of the programme
		Improved relationships: Of those needing support for improved relationships, there is an increase in the number reporting an improvement at the end of the programme

	Improved family dynamics: Of those needing family support due to family conflict or risk, there are improved family dynamics and safety factors by the end of the programme
	Improved work-related skills, knowledge and employment: Of the number requiring support, there is an increase in the numbers accessing and sustaining engagement in education, training and /or employment (ETE)

There are long term outcomes that may arise because of London Gang Exit, but due to timescales, it is unlikely they will be measurable.

- assess the progress and effectiveness of a service they have jointly commissioned.

2.3.2 The intended effect on the individual

Data should be used to ensure the subject's risk of serious harm to the public or themselves is reduced. The evaluation will contribute to the evidence base of 'what works' in gang/serious violence interventions. Information used by MOPAC will be depersonalised at the earliest opportunity and reported at the aggregate, not an individual level and not used in a way whereby an individual can be identified by any means (e.g. reporting on data with small base sizes). This includes (where relevant) survey or interview answers; crime and victim data; and staff information. Reporting may take the form, but not be limited to: internal written documents or briefings; data visualisation packs or dashboards; info-graphics; journal articles or published documents; and may include case studies or quotes from research participants.

2.3.3 Broader benefits of processing data

This document deals with the need to process PII within the London Gang Exit evaluation, enabling MOPAC to:

- See if the service has been a 'success' (See 2.3.1)
- Feeding PII informed analysis into the evidence base will ultimately have substantial benefits for communities (all publicly disseminated findings will be appropriately sanitised and presented at aggregate level); individuals and bespoke groups. However, risks to individuals must be considered and controlled for. As a significant amount of personal and sensitive data will be processed, analysed and used for research purposes by E&I, there is a substantial potential risk to individuals. Risks are documented, and where possible mitigated, in this document.
- The programme will make a significant contribution to the existing knowledge base on gang interventions for children and young people who have experienced gang related harms within the UK.

3 CONSULTATION AND STAKEHOLDER AND ENGAGEMENT

The following stakeholders have been consulted on this DPIA. They include:

1. MOPAC – MOPAC's Criminal Justice & Commissioning Team (Gangs/Serious Youth Violence team) and Data Protection Lead
2. Safer London – Lead delivery partner

MOPAC will continue to engage with the Information Commissioner's Office to ensure the project is compliant with current GDPR.

3.1 Describe when & how you will seek views, or justify why it's not appropriate to do so

For the evaluation, as a rule the engagement of relevant partners will be encouraged, to assess views; the extent of risk; and find appropriate mitigation. All relevant organisations involved in the delivery of the service will regularly be updated with research plans – this includes at multiple internal meetings such as programme board and the delivery team meeting.

3.2 Who else do you need to involve in your organisation?

A number of MOPAC employees require input into this document:

- Programme Lead (Policy) – [redacted]
- Young People and Violence Lead – [redacted]
- E&I lead – [redacted]
- E&I LGE evaluation lead – [redacted]
- GDPR lead – [redacted]
- Data Protection Officer – James Bottomley
- SIRO – Paul Wylie

3.3 Do you need processors to assist?

There should be no requirement for processors to assist, except for:

The already contracted ORS will be used as a processor to obtain online survey responses (see contract Ref: SS31380).

Contacted processors will not have access to the CMS data extract or any other stakeholder PII (e.g. MPS data).

3.4 Do you plan to consult information security experts or any other experts?

Where appropriate E&I will engage with the MPS to ensure internal security specifications are followed.

Legal

Section 4: Necessity and proportionality

This section of the DPIA explores the legality of the sharing activity and how the agreement will comply with the relevant legal and official authorities. This includes when processing PII; special category data; and criminal offence data and will state the compliance with Article 6 (and Articles 9 and 10 where required) of the GDPR and the Data Protection Act 2018.

4.1 What is your lawful basis for processing?

The lawful bases for processing data are: contract, legal obligations, vital interests, public task and legitimate interests. Data for the evaluation will be processed under a different lawful basis depending on the source. Please below for details.

4.1.1 Lamplight (CMS)

As MOPAC commissioned a service for victims, the access to the associated service data is being done under as a disclosure from the programme data controller to MOPAC, who will then act as a data controller for the evaluation data received. MOPAC can rely on its 'public task' justification under Section 143 of the Anti-Social Behaviour, Crime and Policing Act 2014. Under GDPR article 6(3) public

task means: “the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law”.

The programme data controller, Safer London, will document their lawful basis for sharing the data with MOPAC.

MOPAC E&I process data under Section 143 of the Anti-Social Behaviour, Crime and Policing Act 2014 because MOPAC may provide or arrange for the provision of (a) services that in their opinion will secure, or contribute to securing, crime and disorder reduction in the body's area, and/or (b) services that are intended by MOPAC to help victims or witnesses of, or other persons affected by, offences or Anti-Social Behaviour (ASB). The E&I evaluation of LGE will directly assist in the provision of services to reduce gang-related offending or potentially other crimes and/or help victims, witness or members of the public affected by these offences.

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. To lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

In addition to PII MOPAC E&I will also be processing special category data, potentially:

- race
- ethnic origin
- health (including mental health)

Along with the public task access under S.143, MOPAC E&I will be using the Article 9 special category (g) ‘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’, to access this data.

4.1.2 Metropolitan Police Data

When accessing MPS data, MOPAC relies on its statutory responsibility and core oversight function (see ISA REFXXX).

For the LGE project analysis will utilise criminal offence data held on Crime Reporting Information System (CRIS), the gangs MATRIX and Police National Computer (PNC) data, to understand an individual’s offending and victimisation before and after engaging with the LGE programme. The comparison group to measure impact may also be taken from these systems.

To process MPS generated PII MOPAC E&I will rely on its ‘public task’ justification under Section 143 of the Anti-Social Behaviour, Crime and Policing Act 2014 (see 4.1.1 Lamplight CMS – as MOPAC commissioned the LGE service and MPS data will be used to evaluate the service intended to the reduction of offending and help victims of crime and ASB.

To fulfil the requirement of the GDPR for a separate condition for processing criminal offence data under Article 10:

Personal data relating to criminal convictions and offences or related security measures may only be processed:

- *under the control of an official authority; or*

- *when permitted under EU or Member State law.*

Any comprehensive register of criminal convictions may be kept only under the control of official authority. Member States may impose restrictions on the processing of personal data for the purposes of enforcing civil law claims.

MOPAC E&I access criminal offence data in their official oversight authority under the Police Reform and Social Responsibility Act 2011. Analysing this data through the MPS systems negates the need for the LGE to obtain data not required for the everyday running of the service, therefore adhering to data minimisation principles.

4.1.4 Bespoke evaluation data – primary data collection
Wherever possible data primarily collected throughout the evaluation (e.g. via surveys and interviews) will not be PII and therefore not require justification for access under the GDPR. However, MOPAC E&I will seek permission from professionals or service users/family members to gather their feedback.

MOPAC E&I rely on its 'public task' justification under Section 143 of the Anti-Social Behaviour, Crime and Policing Act 2014. Under GDPR article 6(3) public task means: "the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law". MOPAC's basis under Section 143 of the Anti-Social Behaviour, Crime and Policing Act 2014 is because MOPAC may provide or arrange for the provision of (a) services that in their opinion will secure, or contribute to securing, crime and disorder reduction in the body's area, and/or (b) services that are intended by MOPAC to help victims or witnesses of, or other persons affected by, offences or Anti-Social Behaviour (ASB). The E&I evaluation of LGE will directly assist in the provision of services to reduce gang-related offending or potentially other crimes and/or help victims, witness or members of the public affected by these offences.

As no PII will be stored with this information, MOPAC E&I cannot remove data or omit it from analysis once it has been collected. Participants will be informed of this at the outset of their involvement in the research. If there is a potential for PII to be processed MOPAC E&I will seek consent and this DPIA will be updated accordingly.

4.2 – Does the processing actually achieve your purpose?
Yes – the processing will enable oversight of the programme and provide the best possible chance of demonstrating a measurable impact.

4.3 – Is there any other way to achieve the same outcome?
Using non-PII would affect the ability to demonstrate any potential impact on an individual offending and victimisation patterns, which is a key outcome for the project.

It is also the best possible chance of demonstrating 'success'. This is because other measures will potentially not be sensitive enough to register an impact over the course of the pilot or are more subjective in their nature (e.g. LGE distance travelled scale and personal satisfaction with the service or indicative opinions).

Capturing the criminal justice data available from the MPS systems on the CMS is dismissed, not only for cost and resource implications, but because it would mean storing MPS derived PII on an external system. This has security implications and does not adhere to data minimisation principles – as the LGE providers do not require access to this.

4.4 – How will you prevent function creep?

The evaluation plans are documented and have been reviewed. The 'gold standard', or best possible evaluation has been described and therefore outlines all the processing deemed necessary to conduct robust research. The likelihood is, that due to data quantity/quality, less processing will occur than originally described.

The evaluation will produce products at key milestones which will be reviewed internally and by partners. This will ensure plans are on track and there is no deviation from what has been outlined in this document.

4.5 – How will you ensure data quality and data minimisation?
Access to the CMS data is restricted to SL staff, therefore MOPAC do not have direct access. A pre-determined data extract will be provided, and this has been limited to adhere to data minimisation.

As described above the use of CJ data on the CMS system has been dismissed and the reasons for this include adhering to data minimisation.

If MOPAC E&I believe there are errors in the data they will contact the authors (SL) to clarify and/or rectify the information.

4.6 – What information will you provide to individuals and will you ensure they understand it?
As detailed in Section 2.3.2, Safer London have developed a privacy notice issued to clients that wish to take part in the LGE programme. The document provides – in age appropriate language – relevant pre service information including how data will be used and for what purposes. Steps have been taken to address an identified transparency issue in ensuring that MOPAC are explicitly cited as programme commissioners and MOPAC E&I are evaluators.

SL documentation outlines the information provided to service users at different stages of their contact with the service. This will include information in age appropriate formats and for those with additional needs or vulnerabilities. Any direct contact with service users for the evaluation will adhere to the principles set out in the overarching DPIA. Contact with stakeholders/professionals includes information at the first point of contact, outlining the research aims and their rights.

4.7 – How will you support their rights?
The evaluation will follow any specific rights set out in the SL service agreement. Service users will be informed of their rights when initially accessing the service. Any clients partaking in interviews will be informed of their rights to provide consent; withdraw their consent; and access data held upon them (see Section 5.3 Subject Access Requests). As described above, amendments have recently been made to the Privacy Notice issued to prospective service users to explicitly list MOPAC as commissioner. Individuals already on the service have been contacted and informed of change. All individuals are given an option to opt out.

MOPAC E&I will ensure the right for individuals to not be identified personally (or through any means where this is possible e.g. small base sizes) in any publications/written documents and will adhere to all other parts of the GDPR relating to data processing; storage; retention and deletion set out in this document.

4.8 – What measures do you take to ensure processors comply?
MOPAC are responsible for ensuring the security controls are implemented and MOPAC staff are aware of their responsibilities under GDPR 2018 legislation. Compliance with these security controls will be catered for in the periodic reviews of the DPIA. MOPAC (not the MPS) have responsibility for

the conduct of MOPAC staff within the MPS systems and the MOPAC data within the FOUNDATION system – e.g. flagging where personalised data is stored and retained within Shared Drive on the asset register.

All MOPAC staff using FOUNDATION may be subject to regular MPS Department of Professional Standards checks on the use of MPS systems to ensure use is proportionate and legal. Where there are reasonable grounds to suspect an employee's use of MPS systems may not be proportionate and legal, the line manager will liaise with the Information Assurance Unit and DPS. Any issues concerning compliance with security measures will form part of the reviews of this agreement. MOAPC agrees where necessary to allow peer-to-peer reviews to ensure compliance with the security section of this ISA. Compliance with these security controls will be catered for in the periodic reviews of the ISA.

There are no other plans to use contracted processors for this project. If this changes a Data Processing Agreement or Contract will be completed and this DPIA will be updated accordingly with the relevant references.

4.9 – How do you safeguard any international transfers?
Data Protection legislation states that PII shall not be transferred to a country or territory outside the European Economic Area, unless it is in the public interest and that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data. MOPAC confirm the information for the LGE evaluation will remain within the EEA. If a need ever becomes apparent to share PII outside the EEA, MOPAC will liaise with all partners and update this DPIA.

5 Roles and Responsibilities

5.1 – Who are data controllers and who are processors for the project?

The Data Protection Act (DPA) draws a distinction between a 'Data Controller' and a 'Data Processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the Data Controller that must exercise control over the processing and carry data protection responsibility for it.

A 'Data Controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be processed.

A 'Data Processor' in relation to personal data, is any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller. Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- *organisation, adaptation or alteration of the information or data;*
- *retrieval, consultation or use of the information or data;*
- *disclosure of the information or data by transmission, dissemination or otherwise making available; or*
- *alignment, combination, blocking, erasure or destruction of the information or data.*

The key relationships for the London Gang Exit programme have been described in the introduction.

- MOPAC is the commissioner of the service, and also a controller of PII (only for specific PII data outlined in this document). Processing of this data is solely for the purpose of conducting the LGE evaluation.
- Safer London is the lead delivery partner for the intervention and is joint controller of the LGE data, including that which is provided to Safer London by the MPS, CRC, DWP and Catch-22 (TTG Resettlement Services).
- DWP/CRC are delivery partners and sub providers for the LGE programme, they have embedded staff who provide agreed data to SL under SL information governance agreements.
- Catch-22 is a delivery partner for LGE. PII data shared with SL by Catch-22 is covered in the 'Catch-22 Referral Agency Agreement – Effective from 25/05/2018 – 21/04/2022'. Under the terms of this agreement SL becomes the data controller for PII data shared by Catch-22.
- Opinion Research Services (ORS) is MOPAC's contracted processor for online surveys.
- MPS are controllers of MPS data. MPS data accessed by MOPAC for evaluation purposes does not get disseminated to SL or any other organisation expect for in aggregated, sanitised form in terms of evaluation findings. The MPS are a sub provider to SL (to inform referrals); this is covered in 'Data Sharing Agreement between MPS and Safer London – May 2018'.

Each Data Controller has full responsibility to process the shared personal data lawfully, safeguard any personal information or data to which they have access and to ensure, where appropriate, confidentiality.

5.2 – Do all parties understand their role and responsibilities as a controller or processor?
The communication processes for division of responsibilities and risk for the LGE programme are documented in the Safer London Information Governance documents (e.g. Safer London Information Sharing Policy v. Aug 2018; Data Protection Policy v. Nov 2018; Data retention archiving and deletion v. 1b November 2018).

5.3 – How will Subject Access Requests be handled?
Individuals have the right to request certain aspects of data held on them, by making a Subject Access Request (SAR). MOPAC's private office is the single point of contact for SARS, but in the case of LGE the expectation is requests will go to the service delivery organisation (e.g. Safer London). The processes for dealing with Subject Access Requests, Freedom of Information Requests and issuing a Fair Processing Notice are stipulated by SL and MOPAC. It is recognised that any of the organisations involved with London Gang Exit may receive a request for information made under the Act that relates to the operation of this agreement. Where applicable, they will observe the Code of Practice made under S.45 of the Freedom of Information Act 2000. This Code of Practice contains provisions relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the information requested. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to information they do not hold.

For any requests made to MOPAC the below processes will be employed as soon as possible on receipt in order to comply with the statutory time limit:

- When MPS data is processed by MOPAC any rights to request access such as: Freedom of Information Requests; the right to delete etc will follow MPS processes and be passed back to the MPS as authors of the data.
- When bespoke LGE CMS data is processed by MOPAC under the label of 'joint controller' any requests will be passed back to the author of the data – e.g. the lead provider of Safer London.

- When bespoke project data is processed by MOPAC under the label of 'Controller' (e.g. staff interviews or data collected by E&I) any requests will be passed to the MOPAC Data Protection Officer

5.4 – How will data breaches be minimised and dealt with if one occurs?
MOPAC has a data breach procedure which stipulates that any ICO defined notifiable data breach will be reported to the ICO within 72 hours of the breach occurring or being detected. For MPS data, MOPAC will also report ICO defined notifiable breaches to the MPS representative (the Information Assurance Unit) within 24 hours by emailing the 'IAU Mailbox - Security Incidents'. For Child House CMS data MOPAC will also report ICO defined notifiable breaches to the lead provider representative within 24 hours.

On being notified of a possible incident, the stakeholder organisation must establish how significant it is. Some of the factors to consider include:

- the nature of the information (is it personal information or sensitive corporate information?)
- the number of individual records involved (if personal information)
- the possible impact of the incident, including the apparent risk to the individuals, their families, staff, members of the public and MOPAC's operations or reputation;
- the necessary actions to be taken to mitigate the risk, both immediately and for the future.

If the incident is considered serious or impacting, the lead manager must immediately inform the appropriate Senior Official through the management line. An investigation should take place into the circumstances of the loss to ensure that lessons are learned and shared where necessary.

MOPAC will ensure E&I staff follow the data storage principles set out in this agreement, to safeguard the security of electronic data. All MOPAC staff using FOUNDATION are expected to follow the MPS Information Code of Conduct.

In the event of misuse of data being identified, line managers will liaise with the MPS and/or Safer London. Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures of MOPAC. If misuse is found there should be a mechanism to facilitate an investigation into initiating criminal proceedings where that is considered appropriate and necessary.

Formal termination procedures must be implemented to help protect organisations from potential lawsuits, property theft and destruction, unauthorised access or workplace violence. MOPAC has procedures for various scenarios including resignations, terminations, layoffs, accident or death, immediate departures versus prior notification and hostile situations. All parties to this agreement will ensure their Exit Strategy includes appropriate consideration of the following:

- Surrendering keys, security badges and parking permits
- Conducting an exit interview (or 'exit form' for employees)
- Security escort to collect one's personal belongings and/or to leave the premises
- Returning company materials (notebook computers, mobile phones, PDAs etc) Customised arrangements may need to be made for staff who usually work from home or who are temps, contractors or consultants
- Changing door locks and system passwords
- Formal turnover of duties and responsibilities

- Removing network and system access and disabling user accounts
- Policies regarding retention of e-mail, personal files and employment records
- Notification of customers, partners, vendors and contractors, as appropriate.

All partners are responsible for ensuring the security controls are implemented and staff are aware of their responsibilities under the Data Protection Act 2018. All partners to this agreement will provide a list of contacts to deal with queries and requests for information under this agreement. The organisations will also nominate persons to act as the secondary contact to ensure continuity in the absence of the original points of contact.

6 RISK ASSESSMENT

Principles	Identified Risk	Level of Risk	Mitigation
Data minimisation	MOPAC collects a greater level of detail than that which is strictly necessary	Medium	All processing is specific and tailored to the aims and objectives of the project. *The Lamplight CMS* • The data fields stipulated for collection on the bespoke Lamplight CMS for the evaluation have been devised in consultation with providers and professionals. • The majority of data fields that will be used in the evaluation are tick boxes rather than free text responses to minimise the level of data captured. *The MPS Systems* • The MPS data will only be accessed for the purposes of identifying pre and post victimisation and offending. It is unlikely any other MPS system will be used, except for MERLIN records that focuses on vulnerability. • For this project MOPAC E&I will not be providing any information to any other partner - including back to the police. • By E&I accessing MPS data directly, this negates the need for CJS data, not needed for the management of LGE, to be stored on the CMS. *Bespoke Data*

			• Semi-structured interview schedules will be project specific, e.g. focussing specifically on implementation and delivery. For interview/surveys/focus groups the subject will be notified on induction of the use of all whereabouts data and permission to take part will be sought.
Storage limitation	Partner agencies do not follow MOPAC/ Safer London data retention policies and do not delete data at the end of the project	Low	All parties carrying out the functions set out in this DPIA must adhere to their organisation's record management policies and procedures specifically in relation to retention and destruction of data. Such policies and procedures must be DPA compliant. Once the pilot and the evaluation process has concluded MOPAC will review the need of retention of data for historical research purposes. MOPAC E&I will follow the retention policies set out in the ISA Ref: MOPAC/MPS/2018/01
Purpose limitation	Use of data for evaluation is unlawful	Medium	MOPAC's Evidence and Insight Team have been commissioned to undertake the evaluation. MOPAC's Evidence and Insight Team have Metropolitan Police Service accounts and therefore all data is transferred via secure email and is stored on a secure server. All Evidence and Insight employees are Counter Terrorism Clearance security checked. The evaluation of the programme is an extension of the lawful basis as it is required to understand whether the programme works. MOPAC's Evidence and Insight Team will abide by MOPAC's Information Governance Policy. Further lawful basis are provided for

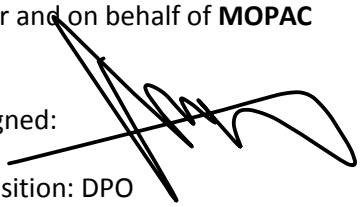
			different types of data access (e.g. consent – see Legal section 4).
Storage Limitation	Loss or compromise of data	Medium	All stakeholders must follow their local policies on reporting a compromise or loss of data (see section 5.4). An investigation should take place into the circumstances of the loss to ensure that lessons are learned and shared where necessary.
Lawfulness, fairness and transparency	Clients have a lack of understanding around the use of data	Medium	The key identified risk around updating the Privacy notice to explicitly name MOPAC as a commissioner, and the requisite updating of current service users of this change is underway. This DPIA will be updated when this task has been completed and well ahead of data use in the final evaluation.
Accuracy	Inaccurate data recording	Low	SL are the authors of all data inputted by the health and care team and therefore responsible for the accuracy of the LGE data entered by the health and care team. For data obtained by MOPAC E&I (i.e. survey responses and interview transcripts), a QC-ing process will take place to ensure the accuracy of the records.
Integrity and confidentiality	Agencies without permission view LGE data; Risks to MOPAC – reputational and financial	Medium	Data will only be shared when necessary, justified and proportionate to do so. As stated MOPAC E&I will not be sharing individual level data with any organisation without the prior consent of the data authors, Safer London (see Section 2: data sharing) Stakeholders must make themselves aware of, and adhere to, their organisation's information security policies and

			procedures in regard to handling data in a manner appropriate for the assigned Government Protective Marking, which will usually be Official or Official Sensitive.
Purpose limitation	Access to MPS and PNC data for the evaluation is lawful	High	The Information Sharing Agreement (ISA) between MOPAC and the MPS is currently in draft format and has not been signed off. As part of this process steps are being taken to secure lawful access to PNC data; discussions are currently taking place but this remains a key risk until the ISA is signed off.

5 SIGN OFF

For and on behalf of **MOPAC**

Signed:



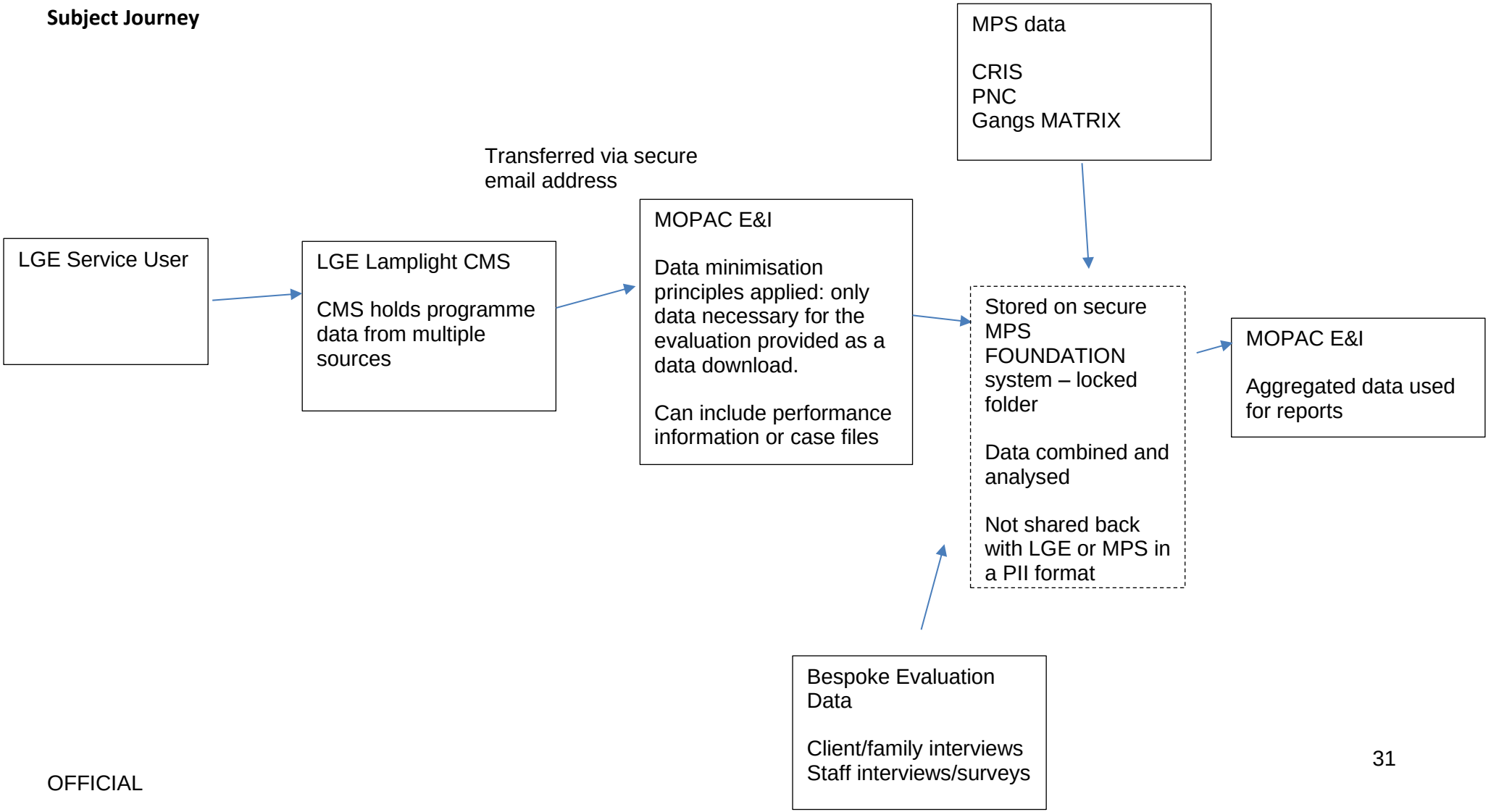
Position: DPO

Date: 26/11/19

6 ANNEXES

Annex A – Data Flow Diagrams

Subject Journey



Annex B – Example of Thematic Data Requirements

Area	**Variable Name**
Personal	Full name
	Home Address - Post Code
	Date of Birth
	Age at Point of Referral
	In receipt of benefits at point of referral
	Immigration Status
	Known to Social Care/Services
	Caring Responsibilities
	Dependents
	Living/Accommodation Status: At Point of Referral
	Living/Accommodation Status: Current
	Gender
	Ethnicity
	Sexual Identity
	Faith/Belief
Needs#1	Disability/SEN
	Disability type
	Language or communication needs?
	If yes, explain
Case Tracking	Case Status
	Date Client Allocated
	Engaged at 3 months
	Engaged at 6 months
	Engaged at 9 months
	Pre-Initial Closure Detail
	Other
Risk	Current Safeguarding Concern
	Safe to Lone Work
	Current Risk to Self
	Current Risk from Others
	Current Risk to Others
	On the police matrix?
	Police matrix score
	Any convictions?
	Statutory Order
	Victim of weapon enabled crime prior to working with service?
	Details
	Victim of weapon enabled crime whilst on the service?

	Details
Outcome Scores	Gang Involvement
	Offending behaviour
	Safety
	Coping strategies
	Access to housing
	Health & wellbeing
	Relationships
	Family Dynamics
	Engagement in ETE
	Expected End Date
Outputs	Completed Activity
	Housing and Resettlement: Number of moves since start
	ETE: Number of completed activity since start
	Family Support: Number of additional family members supported since start
	Case Closure Status
	Case Outcome
	Case Closure Form Completed
Referral Details	Referral direction
	Referral reason
	Referral notes
	Referral date and time
	Alternate contact details
	Referral success
	Was this a multi-agency referral?
	Is the client aware of the referral
	Referral source
	Referral Borough
	Referral URN
	Date Referral Package sent to Delivery Team
	Known to Statutory Services
	Crime/Environmental Factors
	Family Factors
	Health and Wellbeing Factors
	Young Pesrson's Vulnerabilities
	Young Person's Behaviours
	Experiencing CSE
	Gang Involved or known to gangs
	State gang name if known
	Missing Episodes
	Trafficking

	Domestic Violence in the home
	Experiencing Sexual Violence
	Experiencing Domestic Violence
	ETE Status
	Substance misuse
	Mental health concerns
	Other Factors
	If referred whilst in Secure Estate, state name
	Has client held a tenancy
	LAC Section 20
	LAC Section 31
	Conditional release date
Risk (of referral)	Risk to others:
	Risk to others Details
	Risk from others
	Risk from others Details
	Risk to self
	Risk to self Details
Needs (of referral)	Strand(s)/need(s)
	Strand/need (primary need)
	Why young person should get support under this strand