DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project. **You should only complete this full DPIA where you have been told that one is required by the Information Rights Team or the Data Protection Officer.** If you have not been asked to do a full DPIA please do the pre-screen first. Search on essentials for 'DPIA' and download the DPIA pre-screen.

A DPIA is a legal requirement therefore please complete the form in as much detail as you can so the council has the necessary assurances of data protection legal compliance. Avoid technical language and jargon, and assume little prior knowledge of your subject and project by readers.

Ethics screening: If you have been advised to proceed straight to a full DPIA please complete the ethics screening at the end of this document. If you have already completed a DPIA pre-screen then the ethics screening need not be duplicated.

Project Name	**London Resettlement Partnership (LRP)**	
Project Lead and Information Asset Owner/s	Project Lead	[redacted]
	IAO name and asset	Eve Stickler
Summary of the project. *Outline what your project is about. Start with a general headline and then go into more detail.* E*xplain any acronyms on first use.*	To improve the resettlement outcomes of children from London who enter custody. The resettlement project aims to work with all 10-18 year old children who enter custody (males and females, remanded and sentenced) from all London Boroughs. The overall aim of the project is to work with partners to improve resettlement outcomes for children and reduce reoffending. The project will focus on a number of aims in order to achieve this, these will include: • Define constructive resettlement principles and ascertain how this can work in practice in developing an enhanced constructive resettlement offer. • Identify clear pathways to Release on Temporary Licence (ROTL) (to include ROTL clinics) • Improve education, training and employment outcomes • Develop a pan London accommodation protocol • Work with NHS England and partners to define ways of securing continuity of health pathways from custody to community • Address disproportionality and its impact on pathways to resettlement. • Support local practice networks of resettlement case workers to define improvements and raise strategic issues • Develop a body of effective practice and materials for dissemination nationally to YOTs and other agencies.	

	The London Resettlement Partnership (LRP), reports to the London Accommodation and Resettlement Partnership Board (LARP) and includes the following partners: Youth Justice Board (YJB), Youth Custody Service (YCS), Ministry of Justice (MoJ), Mayors Office for Policing and Crime (MOPAC), London councils, all 32 London Boroughs, the Association of London Directors of Children's Services (ALDCS) and the NHS. Whilst the project includes all 32 London Boroughs, LB Camden is the host for the project. This includes the employment of the LRP Strategic Manager and Project Support Officer, in addition to all administration and commissioning responsibilities for the project. The remaining 31 boroughs are working in partnership with LB Camden and the wider partners (as listed above) and are responsible for jointly agreeing the measures taken within the project to improve outcomes for children in the youth justice system. This is achieved via the London Accommodation and Resettlement Partnership Governance Board and the LRP Steering group on behalf of all partners. In addition, it will be the role of each local authority to monitor the progress and outcomes of the children within their borough and report the data to LB Camden for monitoring, reporting and evaluation purposes as per this DPIA. Additional partners beyond those listed above may be commissioned from time to time to provide bespoke programmes to stakeholders. These include: Spark Inside: to provide life coaching to 10 children residing in HMYOI (His Majesty's Young Offenders' Institution) Cookham Wood and returning to any one of the 32 London Boroughs.
Implementation Date: *Should be at least a month to allow for assessment and any necessary steps to be undertaken*	March 2020 – March 2023 (possible extension) The start date is determined by the time the YJB state on their grant agreement. We have spent the last 12 months confirming our requirements with stakeholders and setting up the project. We have not yet collected any data and have requested a project extension to allow for this time loss.

Initial risk assessment: Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor.

If you have already completed a pre-screen, attach it to the DPIA, skip q1 and go to q2 otherwise please answer the questions below.

Q 1	Step 1: Initial Risk Assessment	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	No
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	No
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	Yes
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	No
1.5	Might the project cause data that was previously anonymous or pseudonymised (where a code is used instead of eg names) to become identifiable ?	No
1.6	Does the project involve multiple organisations, eg public sector agencies eg joined up government initiatives, or private sector e.g. outsourced service providers/ business partners?	Yes
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	Yes
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	Yes
1.9	Will data be combined, compared or matched from multiple sources?	Yes
1.10	Will you process biometric (finger print /facial recognition) or genetic data?	No
1.11	Will the personal data be processed out of the U.K? Eg any provers have out of UK servers?	No
1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	No
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	No
1.15	Will personal data be processed which could result in a risk of if there was a security breach?	Yes
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

Step 2: What personal data is being used?										
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						New/Changed			
							It is a new use as the London Resettlement Partnership and associated YJB Pathfinder are new and have not been in place to request this data before. However, this data is already collated by the YOSs across London and shared with other youth justice organisations. We will be collating this data along with more evidence to gain a better understanding of the needs of London children in order to inform Pan London strategies.			
2.2	**What data will be processed/shared/viewed?** Put a YES in the box as appropriate									
	Personal Data									
	Name	**Y**	Date of Birth	**Y**	Gender	**Y**	National Insurance Number	**N**	Financial Information about the person	**N**
	Address	Y	Email address	N	Telephone number	N	NHS No	N	Other eg a reference number such as Mosaic ref	N
	Other data *(Please state):*			*Please see spreadsheet attached.*						
	Special Categories of Personal Data									
	Racial or ethnic origin	Y	Fingerprints/ Biometrics	*N*	Religious or philosophical beliefs Political opinion					*N*
	Trade Union membership	N	Physical or mental health or condition							Y
	Sexual life or sexual orientation	N	Housing records Social services records	N	Tax, benefit or pension records	N	Employee/HR records			N
	Other data *(Please state):*		See spreadsheet attached.							

		Spark Inside will be undertaking life coaching with 10 children. They will share the children's progress with the LRP via an outcome star. This will show progress across the following elements: interests and activities, hopes and dreams, health and wellbeing, communicating, choices and behaviour. See appendix 1.
2.3	Will it include data about any criminal offence committed or alleged, or criminal offence record?	Yes. Offence data including number of pre-cons, current offence, gravity score, reoffending on licence and breach of licence. Asset Plus documents will be requested for a maximum of 16 individual to enable MOPAC to undertake detailed analyses of a small number of individuals for evaluation purposes. These documents can be anonymised.

Step 3: Describe the data processing		
3.1	**Describe in as much detail what is being done with the data - how is the data being used, how it is being handled, stored and transferred/shared?**	**How is the data being used?** The data will be used to develop a pan London picture of the resettlement experience of children within the youth justice system. At a case level it will be used to identify specific barriers and challenges. Aggregate level will be used to identify system issues and trends that require system change or changes in policy and/or legislation. **How is it being transferred?** The data will be shared using secure file transfer using cjsm. Files will be encrypted and password protected where this is required by different organisations, noting that some organisations cannot accept passworded documents. **How is the data being handled?** Each local authority will share their latest data set on a monthly basis. This data will be input in to a spreadsheet that has restricted dropdown lists wherever possible. The data will be stored securely within the data controller's local systems and be shared via cjsm to LB Camden. Camden as joint data controllers will combine the data with the other boroughs' data. This will only be shared within Camden (with the team working on the project) and with the named evaluators within MOPAC. The data will be used to identify (1) key issues with particular individuals such as housing needs or education needs that need to be addressed to support their resettlement, (2) to develop reports using aggregate data to share with the LARP Board to identify areas of strength or more importantly areas where issues needs to be addressed, where parts of the system may require reform, investment or changes to policy or legislation. **How is the data being stored?** At LB Camden Data will be stored within a closed MS TEAMS group. All files will be encrypted and password protected. Excel will be used to record the data. **How is the data being shared?**

		Data will be shared via an encrypted and password protected excel document. This will be sent securely via a cjsm email between London Boroughs and Camden and between Spark Inside and LB Camden. Once the data from all boroughs has been combined and checked for anomalies, this will be shared with MOPAC (the project evaluators) via a secure email. Again the file will be encrypted and password protected.
3.2	**Explain in as much detail as possible why this is being done**	The YJB and the YCS collate data from YOTs on a monthly basis but this data does not allow us to identify particular trends and barriers to resettlement (e.g., why looked after children are more likely to breach their licence and return to custody, or why young black boys are less likely to access education and what other factors may be impacting on these outcomes). The aggregate data shared by these organisations is not enough. We require both a local (borough level) and pan London picture of the needs and resettlement experience of London children to enable us to better inform systems, processes, policy and practice. This is part of a funded project by the Youth Justice Board, Youth Custody Service and 32 London Boroughs, to improve the resettlement outcomes of London Children, with the overall aim of reducing reoffending. MOPAC are undertaking the evaluation of the project. Spark Inside have been commissioned to deliver 1:1 life coaching to 10 London children. They are specialists in providing life coaching to young adults and children within the criminal justice system.

<table>
<tr><td>3.3</td><td colspan="2">Are you sharing the data with an external organisation or partner or are they involved in processing the data?</td><td>Yes
Case level data will be shared with MOPAC for the purposes of the evaluation.
Outcome Stars for the 10 children undergoing life coaching with Spark Inside will be shared with MOPAC for evaluation purposes. Spark Inside will be collating their own data to identify referrals through HMYOi Cookham Wood, and to monitor and assess the progress of each child whilst they are undergoing life coaching.
MOPAC will request a maximum of 16 Asset Plus documents. These will be selected from the data set they are provided and will be used to build a more in-depth picture of the child for evaluation purposes.
Aggregate data and case studies will be shared with the LARP Board (32 Boroughs, MoJ, YJB, YCS, NHS, ALDCS, MOPAC, London Councils)</td></tr>
<tr><td rowspan="4"></td><td>External organisation or partner
Name</td><td>Controller or Processor?</td><td>Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection ? Yes/No/In progress</td></tr>
<tr><td>Mayors Office for Policing and Crime (MOPAC)</td><td>Processor</td><td>In progress (needs to be in place before work commences)</td></tr>
<tr><td>All 32 London Boroughs</td><td>Controller</td><td>No (we require a DSA between Camden and all boroughs for the purpose of this project).</td></tr>
<tr><td>Spark Inside</td><td>Controller</td><td>In progress (needs to be in place before work commences)</td></tr>
<tr><td>3.4.</td><td colspan="2">Has a data flow mapping exercise been undertaken?
If yes, please provide a copy, if no, please undertake</td><td>Yes</td></tr>
<tr><td>3.5</td><td colspan="2">How will the information be processed/shared. Details eg secure file transfer</td><td>Data will be shared by named individuals via secure email (cjsm). Files will be encrypted and password protected.</td></tr>
</table>

		MOPAC have confirmed that their email address is secure and this has been signed off by IT Security at Camden. Spark Inside will be using a cjsm email address to share all data securely.

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify Lawful Basis for processing personal data/special category /criminal data. Ask IRT for advice if needed (DPA@camden.gov.uk if you have no named Information Rights Officer advising)** **If not processing the category say N/A**		
	Personal data Article 6(1) UK GDPR condition	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition**	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition**
	Personal data: Article 6(1) (c) legal duty and **6(1)(e)** processing is necessary for the performance of a task carried out in the public interest **.** The Crime and Disorder Act 1998 gives each LA in England & Wales has the responsibility to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this. Section 115 of the Act gives partners the power to share information for the purpose of reducing crime and disorder. Schedule 9 (5) of the Police and Justice Act strengthens this by introducing a new duty on the same agencies. The Children Act 1989 Under S.47 of the Children's Act 1989, a Local Authority has a duty to investigate when informed that a child in their area is in police protection or the subject of a protection order. The Children Act 2004, as amended by the Children and Social Work Act 2017, places duties on key agencies in a local area. Specifically, the police, clinical commissioning groups and the local authority are under a duty to make arrangements to work together, and with other partners locally, to safeguard and promote the welfare of all children in their area. The Statutory Guidance - Working Together to Safeguard Children (2018) and Information Sharing – Advice to Practitioners providing safeguarding services to Children, Young People, Parents, and Carers (July 2018) emphasise the need to share appropriately. **Special Category Data: Art 9(g)** Reasons of substantial public interest (with a basis in law) and **(h)** Health or social care (with a basis in law). For art 9(g) the Data Protection Act 2018 Schedule 1 Part 2 conditions are para 6 6 (Statutory and government purposes) and para 18 (Safeguarding of children and of individuals at risk) with the underlying law being that identified in art 6 above; and for art 9(h) the Data Protection Act		

	2018 Schedule 1 Part 1 condition is (2)(2)(e) Health or social care purposes, the provision of social care. The underlying law is the same as for art 6. Criminal Offence Data the processing complies with Art 10, the art 6 condition is as noted above and the Data Protection Act 2018 Schedule 1 conditions are as noted above.	
4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Information Rights Team have advised this is appropriate**	
	Consent is not the legal basis so consent is not required.	
4.3	**How will you ensure data quality and data minimisation- how will you ensure the data is accurate and you are only using the minimum data to achieve your aims?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below	
	See pre-screen	
4.4	**Have individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data (inc the council) cover this use in their Processing Notice online	Yes
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**	
	Yes	
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject	
	No	
4.7	**Data Retention Period - how long will the data be kept?**	
	The London Borough of Camden retention and disposal policy 2020 states that: • R19.2 Youth Offending Service [Retain until 25th Birthday (unless also SEN, LAC, CP] in the first instance. • R28 Looked after Children and Care Leavers [Retain until DOB+ 75 years) in the first instance. For e.g. If the child is also engaged with both above, then the LAC retention period (R28) would override R19.2 for their individual record.	

	Step 5: Information Security Process
5.1	**On what systems will the data will be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*
	LB Camden: The data will be stored via a SharePoint folder within a closed MS TEAMS group. All data will be electronic and saved within a password protected and encrypted Excel spreadsheet.
5.2	**Where is the data stored geographically?**
	Camden's data team are supporting the LRP in developing a closed MS Teams group. This will have a maximum of 5 individuals within the group who will have access to the data.
5.3	**What roles will have access to the information?** (List individuals or staff groups)
	At Camden the following people would have access to the data: • The LRP Strategic Manager • The LRP Project Support Officer • The LAP Project Development Manager • The Director of Supporting People • The Data administrator for the YOS • Spark Inside will have access to their own data only
5.4	Is there role-based access control on all applicable systems? **How will access to information be controlled?**
	Access to the information will be controlled by restricting overall access to the sharded folders. In addition, documents will be password protected and the passwords will only be shared with individuals who need to access the data for processing purposes. Passwords will NOT be shared via email along with the data.
5.5	**Is there an ability to audit access to the information?**
	yes for MOPAC and LB Camden.
5.6	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories data and/or criminal data?**

	Camden has a suite of technical and organisation measures in place as do MOPAC and Spark Inside
5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?**
	Yes. Explored all avenues including London Data Store. Advised to use a closed MS TEAMS group to restrict access and move away from using One Drive. Once files are transferred from the cjsm email to the dedicated folder, the original email should be deleted. All files should be password protected and encrypted. Several meetings have taken place to ensure that Camden Data Team and IT Security are happy with the measures in place. All agreed.

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied).** Assess risk assuming there are no controls in place- controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary. *The completed row is an example. Please delete it when you submit the DPIA*	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
Misuse of data; Personal data could be used in a manner incompatible with the Data Sharing Agreement. This would be privacy intrusive to the data subject and may be processing they would not expect to occur.	Possible	Major	12

Compliance risk: could be a breach of purpose limitation and transparency *Corporate risk*: Reputational risk. Loss of trust from data subjects and the partners providing the data. Legal implications.			
Theft of data; Personal data could be stolen and misused by a malicious third party. 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, unpermitted access by third party / employee, staff not adequately trained, theft of data. *Compliance risk:* personal data could be used maliciously and unlawfully. Safeguarding concerns for individuals involved. *Corporate risk:* reputational risk. Loss of trust. Legal implications.	Possible	Major	12
Loss of data in situ; personal data could be lost, this means that it could have been saved in the wrong area, transferred externally or deleted in error. *Compliance risk:* If deleted in error there is a risk to the project in terms of delivery and effectiveness. If data is lost through incorrect file storage this could lead to malicious or unlawful use by a third party which could lead to personal data about individuals being shared. There would be safeguarding concerns if the latter was the case. *Corporate risk:* reputational risk. Loss of trust. Legal implications	Possible	Major	12
Onward transfer of data ie wider sharing beyond the agreed terms of the DSA; Risk to the safety of personal data if transferred elsewhere. 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 due to lack of physical controls in place *Compliance risk;* personal data could be used maliciously and unlawfully. Safeguarding concerns for individuals involved. *Corporate risk;* reputational risk. Loss of trust	Unlikely	Major	8
Incorrect data shared: Data input at the source is inaccurate or that of the wrong service user. Data corrupted or metadata altered by users.	Possible	Moderate	9

Compliance risk: personal data could be accessed by unauthorised individuals and used unlawfully or for malicious purposes. Safeguarding concerns for individuals whose personal data has been accessed. *Corporate risk;* reputational risk. Loss of trust. Legal implications.			
Data not stored in the correct place; data is not stored on a closed/secure area of the system in an agreed place. The storage area does not have the right level of restrictions in place including limited access or encryptions. *Compliance risk*: personal data could be accessed by unauthorised individuals and used unlawfully or for malicious purposes. Safeguarding concerns for individuals whose personal data has been accessed. *Corporate risk:* Reputational risk. Loss of trust. Legal implications.	Likely	Moderate	12
Data requests not responded to; one or more local authorities do not share information in line with the data sharing agreement or project timescales. *Compliance risk:* project is unable to adequately assess service user needs and support local/regional/pan London with relevant initiatives/policies. *Corporate risk:* reputational risk to the project and inability to guide strategy.	Possible	Minor	6
Data not password protected or encrypted during storage or transfer. This risks the wider sharing of data or data being accessed by third parties for unlawful or malicious use. *Compliance risk*: unauthorised access to data. Personal data of individuals shared leading to safeguarding concerns for service users. *Corporate risk:* reputational risk. Loss of trust. Legal implications	Likely	Moderate	12
Unauthorised access of data: Data is shared with unauthorised third parties and used for something it wasn't collected for, a breach of purpose limitation. Data is accessed from the LRP by those not authorised to have it. For example by an unsecured computer / paper record if printed, or unsecure email etc. Compliance risk: personal data could be accessed by unauthorised individuals and used unlawfully or for malicious purposes.	Likely	Major	16

Safeguarding concerns for individuals whose personal data has been accessed. Corporate risk: Reputational risk. Loss of trust. Legal implications			

Step 7: Identify Measures to reduce risk

Identify measures to reduce or eliminate risks identified in step 6. *Remember that risks need to be reduced to an acceptable level, and not all risks can be eliminated.*

Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by IRT/DPO*

The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.

Risk identified in step 6	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Misuse of data; Personal data could be used in a manner incompatible with the Data Sharing Agreement.	• 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. • Files containing the data to be stored in a closed group within MS Teams with limited access for participants. • Ensure only secure email is used to process the data and password protected documents where required • All parties have codes of conduct for employees and comprehensive polices	Reduced	Low	
Theft of data; Personal data could be stolen and misused by a malicious third party.	• 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. • Data will be saved in a restricted area and all documents will be password protected.	Reduced	Low	
Loss of data in situ; Personal data could be obtained and misused by malicious parties within	• Secure local system will be used to ensure that data is saved in the correct user area. • LB Camden data and IT Security Teams have agreed a safe storage area with limited access. • Organisations involved in the receipt, storage and processing of the data will	Reduced	Low	

the organisation.	agree a safe storage area for all electronic data, with limited access. • All organisations will work inline with their GDPR policies.			
Onward transfer of data ie wider sharing beyond the agreed terms of the DSA;	• Where external transfers are made councils have processes in place to ensure all UK GDPR requirements are met. • DSAs make clear the responsibilities of those working with the data and the limitations of these.	Reduced	Low	
Incorrect data shared: Data input at the source is inaccurate or that of the wrong service user. Data corrupted or metadata altered by users.	• The Data is collected by the Youth Offending Services from tried and tested systems that are used regularly within youth justice to collate accurate and up to date personal information about service users. • Data request uses restricted data entry where possible with the use of dropdown lists in excel. • Data process is set out in data flow chart. • Monitoring by LRP Strategic Manager • Processing of data upon receipt will increase the chance of Camden identifying anomalies which will be raised with the home borough for clarification.	Reduced	Moderate	
Data not stored in the correct place; data is not stored on a closed/secure area of the system in an agreed place. The storage area does not have the right level of restrictions in place including limited access or encryptions.	• Data controllers within the home local authority of the service user will have their own safe and secure systems for file storage. • Camden have agreed a safe storage area with IT Security and the data team. This will be a closed group within MS Team with access limited to a small number of individuals working on the project and within the directorate. • Expectations for all partners will be laid out within the relevant DSA.	Reduced	Low	

Data requests not responded to; one or more local authorities do not share information in line with the data sharing agreement or project timescales.	• Named individuals within each local authority will be identified. • A project support officer is in place to liaise directly with named local authority data leads to ensure data is obtained in a timely manner • There is a central team with well defined processes to handle these	Reduced	Low	
Data not encrypted during storage or transfer.	• All spreadsheets will be encrypted and password protected both for safe storage and file transfer via a secure email. • Password will be agreed with each local authority. These will not be shared via email with the data files. • All staff will have received training inline with GDPR and will abide by their local protocols to ensure safe storage ad transfer of data.	Reduced	Low	
Unauthorised access of data:	• Joint data controllers and MOPAC (evaluators) will have DSAs in place with agreed protocols. • LB Camden will have a contract with Spark inside. • All data to be encrypted and password protected. • Data transfer via secure email only • Limited number o named individuals involved in data transfer and processing. • Agreed data storage areas with limited access. Agreed with IT and data security departments. • Staff involved need up to date training around IT security/GDPR, • Locking of workstations when unattended	Reduced	Low	

	• Ongoing management vigilance to ensure protocols are followed.			
Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*				
Moderate				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? **If not, name of IRO**	No, Sarah Laws Data Protection Manager
DPO advice	
Information Asset Owner acceptance of residual risks	Names of IAOs
This DPIA will kept under review by: (*usually the author or the IAO)*	[redacted]

Version Control

Version	Reason	Date	Author(s)
1.0	New DPIA	August 2022	[redacted] and Sarah Laws
1.1	Amended to include Spark	November 2022	[redacted] and Sarah Laws

Appendix 1
Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Willful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services
Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

IMPACT	Score:		PROBABILITY				
			Rare	Unlikely	Possible	Likely	Almost Certain
		Catastrophic	5	10	15	20	25
		Major	4	8	12	16	20
		Moderate	3	6	9	12	15
		Minor	2	4	6	8	10
		Negligible	1	2	3	4	5

Table 4: is the risk level acceptable?

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required

Appendix 2: Ethics screen.

Only complete this if you have skipped the DPIA pre-screen and proceeded straight to a full DPIA. If you did the ethics screen as part of the DPIA pre-screen ignore this section.

Ethical Assessment. In assessing ethics you need to take into account the benefits, proportionate use, possible biases and transparency of the impact of the proposed processing and analysis of personal data on individuals and groups. It is the responsibility of the Project Manager and Sponsor to assess the potential ethical impacts that the intended processing may pose. (These answers can be reused for questions dealing with the same issues in the Full DPIA if the outcome of this pre-screen requires you to do one) The Data Charter is here: Camden's Data Charter - Camden Council

1. *Effects on Residents*

a) *How does use of this data benefit our residents? (Is there evidence of this approach being likely to meet a public need?)*

This data will benefit the wider community by ensuring that the right opportunities are in place and barriers to resettlement are removed. The overall aim is to reduce reoffending across London meaning fewer victims, more children and young people positively contributing to society and long-term fiscal savings for reinvestment in services.
Cost saving from previous projects show savings for the NHS, DWP, Local Authorities, Police and Probation, all of which could be reinvested to support the wider community.

b) *What would be the harm in not processing this data?*

Harm will be to the children on the cohort as barriers to resettlement may not be identified in a timely way.

For aggregate data, harm may result from not having the correct supporting information to commission the right services or work with partners to get the best outcomes for the child.

At a social level we will continue to have more victims of crime.
Children in London are more likely to be in custody than in any other region in England. There are nearly twice as many in custody than would be expected given the size of the population. If we do not address this problem through projects such as these we have no way of reducing the numbers of children who offend. We also run the risk of young people experiencing a lifetime of crime and placing pressure on adult services including the NHS, DWP, Police, adult prison and probation services.

In 2018-19, London had 247 children, up to and including age 18, in custody, out of a total of 858 in England and Wales. The ethnic breakdown of children in custody shows a disproportionately high representation of children from a BAME background at 78%. As the number of children in custody has

fallen nationally, the proportion who are from BAME backgrounds has increased. London is the major contributor to this disproportionality. These children have often experienced chaotic and traumatic childhoods, many with neglect, rejection or abuse and often present with significant mental health issues. We must work together to tackle these issues.

2. *Data Bias*

a) *How do you plan to identify errors and biases in data collection, analysis and algorithms?*

Data collection fields will be limited where possible to ensure that only relevant data is entered in the spreadsheet. This will be achieved with drop down menus where possible.

Much of the data can be collated from a wizard from existing portals such as child view.

Analysis will only be undertaken by a restricted number of individuals responsible for overseeing the project (e.g., Project Manager, Project Support Officer, Evaluators).

Possible errors will be highlighted to the data owners by the Project Manager and Project Support Officer.

Upon receipt of the data (monthly over the course of the project), the project manager or project support officer will immediately highlight any data errors or anomalies to the data owner for clarification.

For reporting and evaluation purposes caveats can be included to issue caution if necessary and comparisons can be made where possible against nationally published data from the YJB and YCS.

b) *Once errors and biases have been identified in data collections, how will they be taken into account for any future policy or service which uses this work as an evidence base?*

Data collection fields will be limited where possible to ensure that only relevant data is entered in the spreadsheet. This will be achieved with drop down menus where possible.

Much of the data can be collated from a wizard from existing portals such as child view.

Asset Plus requests will be forwarded to MOPAC for evaluation purposes. These will not be altered and will include only the original case notes from the case manager.

Analysis will only be undertaken by a restricted number of individuals responsible for overseeing the project (e.g., Project Manager, Project Support Officer, Evaluators).

Possible errors will be highlighted to the data owners by the Project Manager and Project Support Officer.

Upon receipt of the data (monthly over the course of the project), the project manager or project support officer will immediately highlight any data errors or anomalies to the data owner for clarification.

For reporting and evaluation purposes caveats can be included to issue caution if necessary and comparisons can be made where possible against nationally published data from the YJB and YCS.

c) *Who could be negatively affected by processing this data?* (How can you show there is a **fair balance** between the **rights of individuals** and the **interests of the community**?

The children on the cohort could be negatively affected if the data is lost or shared with the wrong people.

Partners such as the Youth Offending Services, secure estate, YCS and YJB could face reputational damage if the data is not handled and reported sensitively. All partners will be consulted on reporting before anything is shared widely or published.

The interests of sharing this data far outweigh risks to individuals on the cohort as illustrated above. Information of this type is already regularly shared with the youth justice partners/agencies involved.

- *Limitations of Data*
- *How will you make sure that you only process the data that is necessary and proportionate for the purpose of the project, and no more than is necessary?*

The data ask is based on comparisons with previous projects and in consultation with the Youth Offending Service, Youth Custody Service, NHSE and Youth Justice Board. It will continue to be reviewed until all parties are satisfied that we are collating only the data that will benefit individuals and planning/execution of the project.

MOPAC are using their data teams to support monitoring and evaluation and will be part of this consultation process.

- *How are you ensuring the data used is reliable? (**Data quality**)*
- *What processes do you have in place to ensure maintenance of data accuracy? (**Data integrity**)*

Data will be collated at a local level by professionals within the Youth Offending Service who collate data of this type for the YJB on a monthly basis. Where possible data owners will be able to use a wizard to pull accurate information from existing systems.

- *How have you clearly marked origins and destinations of data used to trace source of errors? (**Data lineage**) (Are all metadata and field names clearly understood)*

Guidance will be provided with the data sheet.
Sources of errors will be clearly identifiable by YOT and can therefore be addressed easily.
Data will be shared using an Excel spreadsheet and this will be encrypted and password protected.
Drop down menus and lists will limit the data entry where possible to ensure that it is accurate and we only obtain the necessary information.

Data access will be limited via the following:

- Data owner in home LA: a named individual will be identified within each LA to provide the data.
- This will be sent to the joint data owner at LB Camden via a cjsm email.
- The data will be transferred to a relevant folder within a closed MS TEAMS group for processing.
- A small number of people within with Camden's Supporting People Team will have access to the data. (maximum 5).
- The LRP Project team (2 individuals) will be responsible for checking the data to see if there are any anomalies, raising any questions with the LB who owns the data, and aggregating the data to produce reports.
- Raw data will be shared via a secure email with MOPAC for evaluation purposes. Once the data from all boroughs has been placed in one document, this will be shared as a single file via a secure email.

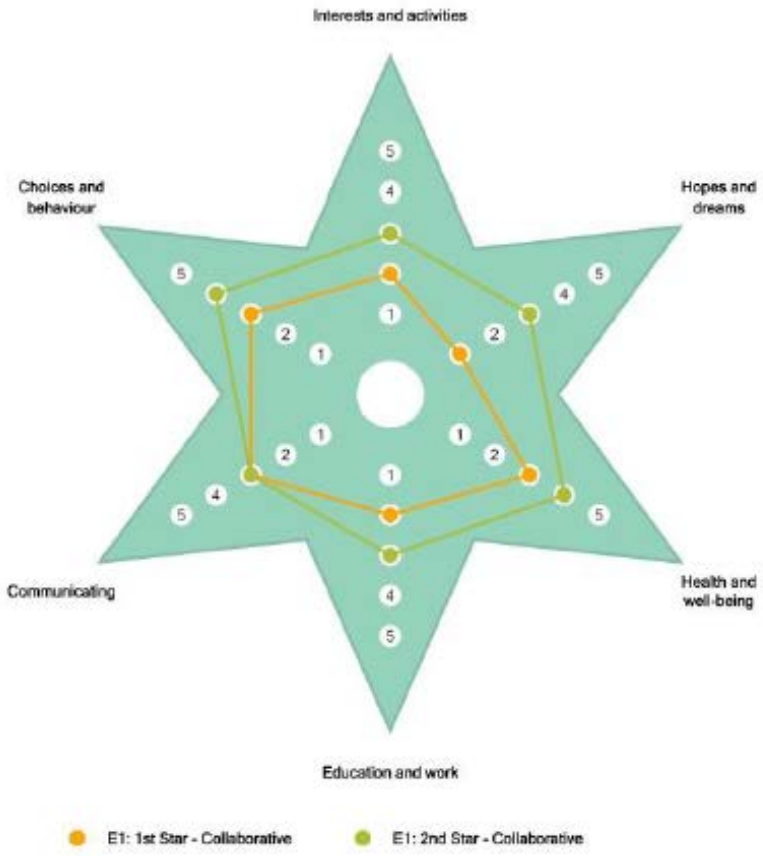
- *How could the objectives of this project be completed without processing the data?*

  We could use aggregate, published data from previous years but this does not enable us to develop a specific offer for London, not does it show emerging trends and challenges. Without this we could not ensure that we are commissioning the right services or developing a resettlement offer that is appropriate for the children of London.

  Without case level data we would not be able to identify barriers and challenges in real time and monitor other contributing factors to these barriers. i.e, identifying that a looked after child does not have suitable accommodation prior to release from custody. At present there is no single functions that provides an overview of resettlement cases across London

Appendix 1

CURRIE-T-HJ-HDN-APR-23



1st Star: 27.4.23

2nd Star: 19.7.23