# 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.

Version Control

| Version | Reason | Date | Author(s) |
|---|---|---|---|
| **1.0** | **New** | **June 2022** | [redacted] **(LB Camden)** |
| | | | |

| | | |
|---|---|---|
| **Project / Work Stream Name** | **Self-Development Programme** | |
| **Project / Work Stream Lead** | Name | [redacted] |
| | Designation | London Borough of Camden |
| | Email | [redacted] |
| **Overview:**<br><br>**(Summary of the project/work stream)** | The successful contractor will provide a bespoke self-development male programme for those involved within the youth justice system using mental health/trauma-recovery model. Phase 1 of the London Accommodation Pathfinder (LAP) between October 2022 to March 2023 and phase 2 between April 2023- March 2024.<br><br>The small number of males will be subject to Court conditions via Remand into Local Authority Accommodation or Youth Rehabilitation Orders within the Youth Justice System and will be aged between 16 17 years old.<br><br>The contractor will deliver small group sessions of up to 5 males at one time with the flexibility of delivering one to one where required on a weekly basis.<br><br>Self-Development programme outcomes: -<br><br>a. Improving the children's perspective of identity and self-awareness<br><br>b. Enhance the children's confidence and self esteem | |

| | |
|---|---|
| | c. Improve the children's perception of masculinity<br><br>d. Stabilise or improve children's chances of education, training, or employment<br><br>e. Stabilise or improve children's chances of health support<br><br>The self-development programme will comprise of five (a-d) key elements as detailed below.<br><br>a) To adopt a relationship based, personal centered approach to engage children by helping them to increase their self esteem, confidence, and social development.<br><br>b) The delivery of services will take place where is deemed best for the children which include the London Accommodation Pathfinder sites or anywhere assessed as safe within their local community.<br><br>c) To provide weekly updates to the lead workers within the child's professional network<br><br>d) To ensure that all relevant staff members that have contact with the children have the relevant DBS checks and safeguarding training |
| **Implementation Date:** | August 2022 to 31st March 2024 |
| **<u>Environmental Scan</u>**<br><br>**Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.** | The contractor will be an established organisation that work with many Youth Justice Services in London delivering similar programmes. |

| **Step 1: Complete the Screening Questions** | | | |
|---|---|---|---|
| **Q 1** | **Category** | **Screening question** | **Yes/No** |

| | | | |
|---|---|---|---|
| 1.1 | Technology | Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy? | NO |
| 1.2 | Technology | Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business? | NO |
| 1.3 | Identity | Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data? | NO |
| 1.4 | Identity | Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? | NO |
| 1.5 | Multiple organisations | Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners? | Yes |
| **Q** | **Category** | **Screening question** | |
| 1.6 | Data | Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled?<br><br>See glossary of terms | YES |
| 1.7 | Data | Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database? | YES |
| 1.8 | Data | Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals? | No |
| 1.9 | Data | Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources? | YES |
| 1.10 | Data | Will the personal data be processed out of the U.K? | NO |
| 1.11 | Exemptions and Exceptions | Does the project relate to data processing which is in any way exempt from legislative privacy protections? | NO |
| 1.12 | Exemptions and Exceptions | Does the project's justification include significant contributions to public security and measures? | YES |

| | | | |
|---|---|---|---|
| 1.13 | Exemptions and Exceptions | Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation? | NO |

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

**Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.**

| **Step 2: Identify the need for a DPIA** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **2.1** | **Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??** | | | | | | | | New/Changed | | |
| | | | | | | | | | New | | |
| **2.2** | **What data will be processed/shared/viewed?** | | | | | | | | | | |
| | **Personal Data** | | | | | | | | | | |
| | Forename | **Y** | Surname | **Y** | Date of Birth | **Y** | Age | **Y** | Gender | **Y** | |
| | Address | Y | Postal address | Y | Employment records | Y | Email address | | Postcode | Y | |
| | Other unique identifier (*please specify*) | | Telephone number | Y | Driving licence number | | NHS No | | Hospital ID no | | |
| | Other data *(Please state):* | | | | | | | | | | |
| | **Special Categories of Personal Data** | | | | | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Racial or ethnic origin | Y | Political opinion | | Religious or philosophical beliefs | *Y* |
| | Trade Union membership | | Physical or mental health or condition | | | Y |
| | Sexual life or sexual orientation | | Social service records | | Child protection records | |
| | Sickness forms | | Housing records | | Tax, benefit or pension records | |
| | DNA profile | | Fingerprints | | Biometrics | |
| | Genetic data | | | | | |
| | Proceedings for any offence committed or alleged, or criminal offence record | | | | | Y |
| | Other data *(Please state):* | Criminal offence data | | | | Y |
| | Will the dataset include clinical data? (please include) | | | | | **no** |
| | | | | | | No |
| | Will the dataset include financial data? | | | | | No |
| | **Description of other data processed/shared/viewed?** | | | | | |
| | Information will be held by the local Youth Justice Service about pending cases, previous and current alleged offences, and previous convictions. | | | | | |

| | | | | |
|---|---|---|---|---|
| **2.3** | **<u>Business sensitive data</u> not in scope** | | | |
| | Financial | | N/A | |
| | Local Contract conditions | | N/A | |
| | Operational data | | N/A | |
| | Notes associated with patentable inventions | | N/A | |
| | procurement/tendering information | | N/A | |
| | Customer/supplier information | | N/A | |
| | Decisions impacting: | One or more business function | | **Yes/No** |
| | | | | N/A |

| | | | |
|---|---|---|---|
| | | Across the organisation | N/A |
| | **Description of other data processed/shared/viewed (if any).** | | |
| | | | |

| **Step 3: Describe the sharing/processing** | | | |
|---|---|---|---|
| **3.1** | **List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below* | | |
| | Name | Controller or Processor? | Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit |
| | | | Yes / No |
| | London Local Authorities | Controller | YES |
| | Contractor | Controller and Processor | YES |
| | LAP Provider | Processor | YES |
| **3.2** | **If you have answered 'yes' to 3.1 is there an existing ' Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor?** | | Yes/No<br>YES, contract between Camden and Contractor, and there will be a Data Sharing Agreement between the public sector partners |
| **3.3.** | **Has a data flow mapping exercise been undertaken?**<br>*If yes, please provide a copy, if no, please undertake* | | YES, appended |
| **3.4** | **Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?**<br>*If yes, provide a copy of the confidentiality agreement or contract?* | | Yes, Contractor as detailed |

| | |
|---|---|
| **3.5** | **Describe in as much detail why this information is being processed/shared/viewed?**<br>*(For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)* |

All of the children and young people involved in the self-development programme will be current or service users of the Youth Justice Service in North Central and East London and their agreement to participate will be obtained.

The professionals involved will largely be employees of the North Central London and East London Local Authorities. It is anticipated that public sector partners will be joined by a Data Sharing Agreement.

**Baseline data:**

*Deliverable* – A baseline study of the extent and effect of children receiving the self development programme. This will be provided by the contractor linked to their KPI's.

*Purpose* – To provide us with a comprehensive understanding of the children's progress and outcomes of the self-development programme.

**LAP Data transfer:**

**Child Referral to LAP Service**: The referring Youth Justice Service will complete the referral which consist of child's risk assessments and criminal convictions and sends this information to the Contractor via Secure Email.

Contractor will store the child's referral form on a secure system, likely to be their case management system.

**During Self Development Programme:** The contractor will complete feedback to the relevant Youth Justice Service of the referring child within 24 hours of their contact.

**Why is this being done:**

Sharing data on the children accessing the self-development programme will firstly enable the contractor to assess the risks and understand their needs.

The Youth Justice Services required feedback on every child contact as they have a statutory duty to monitor the compliance of each child as part of their court order.

**Step 4: Assess necessity and proportionality**

| | | | |
|---|---|---|---|
| **4.1** | **Lawfulness for Processing/sharing personal data/special categories of personal data?** | | |
| | **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.<br><br>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.<br><br>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.<br>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.<br><br>**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<br><br>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** | **Will the information be processed/shared electronically, on paper or both?** | Electronic | X |
| | | Paper | X |
| **4.3** | **How will you ensure data quality and data minimisation?** | | |
| The nature of this data involves a subjective element in what is timely, proportionate, and necessary to share, and also in risk assessments and judgements. These are mitigated by existing Youth Justice Services and Child Social Care processes (e.g. Risk assessment tools, templates and management counter-signature). The sharing of child information between partners involved in the self development programme is subject to the Working Together to Safeguard Children/Information Sharing Guidance referred to above. The referral process is a straight forward process that mitigates the risk of inaccurate data analysis by a single individual or agency.<br><br>The multi-agency parties are experienced and skilled in judging where the threshold for necessary and proportionate data/information lies in regard to safeguarding children and preventing offending/harm. They will | | | |

| | | |
|---|---|---|
| work in line with existing multi-agency information sharing protocols around this cohort, for example those at Youth Justice Services risk panels There will be peer challenge and accountability to ensure information sharing remains necessary and proportionate. | | |
| **4.4** | **Have individuals been informed about the proposed use of their personal or special categories of personal data?**<br>*For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to residents on their websites?* | Yes |
| | All children will be told how their data will be shared with others in order to make informed and defensible decisions and to track monitor the child's progress throughout their journey. | |
| **4.5** | How will you help to support the rights of individuals? | |
| | Rights will be signposted in the relevant Privacy Notices, and individuals will be supported by professionals who are aware of the data subject rights and who to contact to assist the person in using them. | |
| **4.6** | **Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?** | |
| | Home local authorities of the child will be leading on all SAR requests. Access will also be written into the appointed providers contract. | |
| **4.7** | **Will the processing of data include automated individual decision-making, including profiling?**<br>*If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject* | No |
| | | |
| **4.8** | **Will individuals be asked for consent for their information to be processed/shared?**<br>*If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.* | No |
| | Consent is not the lawful basis for sharing. However, in practical terms agreement of the person is needed as every child referred to the contractor will have agreed to be placed there, including the agreement of their parents/carers. This agreement will be included as part of the court order whilst engaging with the Youth Justice Service statutory duties. | |
| **4.9** | **As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the embedded questionnaire.** | No |

| | | |
|---|---|---|
| **4.10** | **Where will the data will be stored**<br>*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.* | |
| | Local Authorities: Will keep sensitive data on secure network systems and secure case management system<br><br>Contractor: Will keep sensitive data on secure network systems and secure case management system | |
| **4.11** | **Data Retention Period**<br>*How long will the data be kept?* | |
| | Contractor will retain the data for the during of the contract and are required to delete upon expiry of the contract. Local authorities have their own retention schedules and these will apply as necessary. | |
| **4.12** | **Will this information be shared/processed outside the organisations listed above in question 3?**<br>*If yes, describe who and why:* | Yes/No |
| | | No |

| | | |
|---|---|---|
| **Step 5: Information Security Process** | | |
| **5.1** | **Is there an ability to audit access to the information?** | Yes/No |
| | This is covered in the contracts. | Yes |
| **5.2** | **How will access to information be controlled?** | |
| | Between agencies via secure emails or password protected documents as specified by each local authority. Information will only be shared on a needs basis to safeguard or make defensible decisions. | |
| **5.3** | **What roles will have access to the information?** (list individuals or staff groups) | |

- Referring Youth Justice Service case manager
- Contractor manager and relevant staff

| | | | | | | |
|---|---|---|---|---|---|---|
| **5.4** | **What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?** | | | | | |
| | Username and password | X | Smartcard | | key to locked filing cabinet/room | |

| | | | | |
|---|---|---|---|---|
| | Secure 1x Token Access | | Restricted access to Network Files | x |
| | Other: *Provide a Description Below*: | | | |
| | | | | |

| | | |
|---|---|---|
| **5.5** | **Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below:**<br>SLSP is required for new systems.<br>*SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.* | Yes/No<br>No |
| **5.6** | **Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?**<br>*Please explain and give reference to such plan and protocol* | Yes/No<br>N/A |

| | | | |
|---|---|---|---|
| **5.7** | **Is Mandatory Staff Training in place for the following?** | Yes/No | Dates |
| | • Data Collection: | YES | |
| | • Use of the System or Service: | YES | |
| | • Information Governance: | YES | |
| **5.8** | **Are there any new or additional reporting requirements for this project?** | NO | |
| | • What roles will be able to run reports? | | |
| | | | |
| | • What roles will receive the report or where will it be published? | | |
| | | | |
| | • Will the reports be in person-identifiable, pseudonymised or anonymised format? | | |
| | | | |
| | • Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format? | | |
| | | | |

| | | |
|---|---|---|
| **5.9** | **Have any Information Governance risks been identified relating to this project?** (if Yes the final section will need to be completed) | **Yes/No**<br>Yes |

| **Step 6: Identify and Assess Risks** | | | |
|---|---|---|---|
| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| *Note: risks here are risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.* | | | |
| **Loss of data in situ**;<br>Personal data could be obtained and misused by malicious parties within the organisation.<br>Compliance risk; Appropriate technical and organisational measures shall be taken.<br>Corporate risk; Reputational risk. Loss of trust. Legal implications. | Possible | Major | 12- Medium/High |
| **Misuse of data (fair, lawful and transparent)**;<br>Personal data could be used in a manner incompatible with the Data Sharing Agreement/contract. No legal basis for the processing, processing may not be necessary or proportionate. The processing is without a Privacy Notice.<br>Compliance risk; Appropriate technical and organisational measures shall be taken.<br>Corporate risk; Reputational risk. Loss of trust. Legal implications. | Possible | Major | 12 - Medium/high |
| **Theft of data;**<br>Personal data could be stolen and misused by a malicious third party.<br>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. | Possible | Major | 12 - Medium/High Risk |

| | | | |
|---|---|---|---|
| Compliance risk; Appropriate technical and organisational measures shall be taken.<br>Corporate risk; Reputational risk. Loss of trust. Legal implications. | | | |
| **Further transfer of data**;<br>Risk to the safety of personal data if transferred elsewhere.<br>UK Data transferred or stored outside UK e.g. in cloud without adequate safeguards. Backups held outside UK, without adequate safeguards. Staff users send personal data insecurely outside UK due to lack of physical controls in place<br>Compliance risk; Personal data shall be obtained for one or more specified and lawful purposes.<br>Appropriate technical and organisational measures shall be taken.<br>Personal data shall not be transferred outside the European Economic Area.<br>Corporate risk; Reputational risk. Loss of trust | Unlikely | Moderate | 6- Moderate Risk |
| **Data accuracy Inaccurate data collected**:<br>Data corrupted or metadata altered by users. Users forget they have shared files or Files shared/deleted incorrectly<br>Corporate risk; Reputational risk. Loss of trust. Legal implications | Unlikely | Major | 8 -Moderate Risk |
| **Unauthorised access of data:**<br>Data used for something it wasn't collected for, a breach of purpose limitation. Data is accessed from the LAP partnership by those not authorised to have it. For example by an unsecured computer / paper record within the residential home, or unsecure email etc..<br>Compliance risk; Appropriate technical and organisational measures shall be taken.<br>Corporate risk; Reputational risk. Loss of trust. Legal implications | Possible | Major | 12- Medium/High |
| **Data Retention**:<br>Risks that appointed provider will retain data beyond a defined period given in their contract.<br>Compliance risk; Appropriate technical and organisational measures shall be taken.<br>Corporate risk; Reputational risk. Loss of trust. Legal implications | Unlikely | Minor | 8- Medium/High risk |
| **Data subject rights:**<br>Data subject requests are not responded to in required timescales. | Unlikely | Minor | 4- Moderate Risk |

| Step 7: Identify Measures to reduce risk | | | | |
|---|---|---|---|---|
| **Identify likely additional measures to reduce or eliminate risks identified as medium or high risk in step 6** | | | | |
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| **Loss of data in situ** | • Contractor policy and procedures to cover this<br>• Contractor staff training around data protection and GDPR<br>• Local Authority scrutiny and challenge where applicable | Reduced | 9 -Medium | Yes |
| **Data Misuse of data (fair, lawful and transparent)**; | • 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.<br>• Ensure only secure email is used to process the data and password protected documents where required | Reduced | 9 - Medium | Yes |
| **Theft of Data** | • Access to council systems are monitored.<br>• 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. | Reduced | 9- Medium | Yes |
| **Further Transfer of Data** | • All Data is held within the UK and there would be no reason for councils to send data out of the UK.<br>• Where external transfers are made councils have processes in place to ensure all UK GDPR requirements are met | Unchanged | 6- Moderate | No |
| **Data accuracy Inaccurate data collected**: | • The Data is collected by the Youth Justice secure way to Contractor.<br>• Data process is set out in data flow chart.<br>• No data can be downloaded by councils who have read only access | Reduced | 6 - Moderate | Yes |

| | | | | |
|---|---|---|---|---|
| | • This will be monitored by the LAP strategic manager to ensure all services are being compliant | | | |
| **Unauthorised access of data:** | • Clear protocols for Contractor need to be viewed before contract award<br>• Staff training around IT security,<br>• Locking of workstations, security of paper records.<br>• Ongoing management vigilance to ensure protocols are followed. | Reduced | 6- Moderate | Yes |
| **Data Retention**: | • Any data recorded eg nominal status in council records will be subject to council retention periods.<br>• Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared.<br>• This Record of Processing Activity (ROPA) must include the retention period for the data.<br>• All partners must a destruction of records policy in place. Information must not be retained for longer than necessary for the purpose for which it was obtained.<br>• Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.<br>• Retention and disposal will be written in Contractor contract | Reduced | 6-Moderate | Yes |

## Overall residual risk level: Medium

| Step 8: Sign off and record outcomes | | |
|---|---|---|
| **Item** | **Name/date** | **Notes** |
| Measures approved by: | [redacted], June 2022 | |
| Residual risks approved by: | [redacted], June 2022 | |
| DPO advice provided: | Sarah Laws | |
| Risks mitigated appropriately and residual risks proportionate to the aims of the project | | |
| DPO advice accepted or overruled by: | Andrew Maughan, DPO | If overruled, you must explain your reasons |
| Comments: Accepted | | |
| This DPIA will kept under review by: [redacted] | The DPIA will be reviewed by the respective DPOs of each organisation when required | The DPO should also review ongoing compliance with DPIA |