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	May 2021	[redacted] (LB Camden)
1.1	Revised and reviewed	February 2022	Sarah Laws (LB Camden)
1.2	Revised and reviewed	March 2022	Victoria Blyth (LB Barnet) and Sarah Laws (LB Camden)

Project / Work Stream Name	**London Accommodation Pathfinder**	
Project / Work Stream Lead	Name	[redacted]
	Designation	London Borough of Camden
	Email	[redacted]
Overview: **(Summary of the project/work stream)**	The London Accommodation Pathfinder offers a residential alternative to custody for London children. This is a pan-London project, led by Camden, with the first phase in East London and North Central London. It is commissioned to reduce both the disproportionate number of London children going to custody (about twice the national rate) and the racial disproportionality amongst this cohort (78% of whom are from Black, Asian or Minority Ethnic origin). It will offer 5 five bed facilities across London for 16-17 year old male children as a direct alternative to their being remanded or sentenced to custody and support resettlement. The aims of the project are to reduce the number of children experiencing custody, improve their safety, wellbeing and life chances, reduce risks of reoffending and harm, and protect the public and victims. The project has pathfinder status and a £1.03 million YJB/MOJ grant to assist its initial set-up and development up until March 2023.	

	In addition, there has been a number organisations commissioned to work under the Pathfinder umbrella as a partnership. This DPIA sets out how the London Accommodation Pathfinder commissioned organsiations will exchange data and a Data Sharing Agreement will be completed between them and participating Local Authorities. **Participating Local Authorities:** East London Sub Region (Newham, Barking & Dagenham, Waltham Forest, Tower Hamlets, Redbridge, Havering). North Central London Sub Region (Haringey, Barnet, Camden, Islington, Enfield, Hackney) **St Christophers Fellowship:** The appointed provider will manage the accommodations across both subregions of London. They will offer intensive support that is specifically designed for this cohort, with a mental health/trauma-recovery model and a strong education, training and employment focus, whilst also providing the knowledge, skills and monitoring necessary to safeguard residents, staff and the public. **Middlesex University:** The appointed university will evaluation the overall Pathfinder and will seek information from all the commissioned organisations. **Wipers Youth CIC:** Appointed to deliver a self-development programme for the children across both sub regions and will engage and exchange information with St Christophers Fellowship, Local Authorities and Middlesex University. **Street Doctors:** Appointed to deliver first aid and weapons programme for the children across both sub regions and will engage and exchange information with St Christophers Fellowship, Local Authorities and Middlesex University. **Fight for Peace Academy** will be appointed to deliver boxing and fitness sessions but only to the East London sub region accommodation and children. They will engage with St Christophers Fellowship, East London LA's and Middlesex University. **Fitness Education Academy** will be appointed to deliver boxing and fitness sessions but only to the North Central London sub region accommodation and children. They will engage with St Christophers Fellowship, North Central London LA's and Middlesex University.
Implementation Date:	The pathfinder period runs from 01.04.21 to 01.04.23 after which the contract may be extended for a further 3 years.

	The first London Alternative to Custody Accommodation is intended to be operating and live for East London and North Central London local authorities from September 2022.
Environmental Scan **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.**	There is no similar project being undertaken: this is a new initiative.

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?	YES

		See glossary of terms	
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?	YES
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	X	Surname	X	Date of Birth	X	Age	X	Gender	X	
	Address	X	Postal address	X	Employment records	x	Email address		Postcode	X	
	Other unique identifier (*please specify*)		Telephone number	X	Driving licence number		NHS No		Hospital ID no		
	Other data *(Please state):*										
	Special Categories of Personal Data										
	Racial or ethnic origin		X	Political opinion		Religious or philosophical beliefs		x			
	Trade Union membership			Physical or mental health or condition				x			
	Sexual life or sexual orientation	x	Social service records	X	Child protection records			X			
	Sickness forms		Housing records		Tax, benefit or pension records		Adoption records				
	DNA profile		Fingerprints		Biometrics		Genetic data				
	Proceedings for any offence committed or alleged, or criminal offence record									x	
	Other data *(Please state):*	Criminal offence data								x	
	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 Offending 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
	Participating London Local Authorities in East and North Central London	Controller and Processor	YES
	St Christopher's Fellowship	Controller and Processor	YES
	Wipers Youth CIC	Controller and Processor	NO
	Middlesex University	Processor	NO
	Street Doctors	Processor	NO
	Fitness Education Programme	Processor	NO
	Fight for Peace Academy	Processor	NO
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 YES, contract between XX and XX (TBC) and there will be a Data Sharing Agreement between the public sector partners
3.3.	**Has a data flow mapping exercise been undertaken?** *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?** *If yes, provide a copy of the confidentiality agreement or contract?*		YES

3.5	**Describe in as much detail why this information is being processed/shared/viewed?** *(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, young people and families involved in the project and research will be current or recent service users of local authority Children's Services or Youth Justice Service and their agreement to participate will be obtained.

The professionals involved will largely be employees of London Local Authorities or other stakeholders. It is anticipated that public sector partners will be joined by a Data Sharing Agreement.

Statutory partners will play a key role informing and implementing the Pathfinder project. Key partner agencies will include:

- The Police including operational teams and the Offices of Police and Crime Commissioners
- Youth Offending Institutions
- London Local Authorities
- Educational establishments including, colleges and alternative education providers

Baseline data:

Deliverable – A baseline study of the extent and effect of children placed at the LAP. This will be provided by monthly returns by the Youth Offending Services that links to child's outcomes and KPI's. These will be sent to the LAP strategic manager and external evaluator.

Purpose – To provide us with a comprehensive understanding of the children's progress and outcomes across the Pathfinder to allow for targeting resource and identifying emerging good practice.

Practice Evaluation:

Deliverable – An evaluation of project to ensure that outcomes for children, provider service outcomes and Pathfinder outcomes have been met. This will be delivered through stakeholder, children and family focus groups and interviews. Funding is not dependent on evaluation and individuals can choose not to take part in evaluation. Evaluation output will be anonymised.

Purpose – To evaluate (including establishing causal links and impact) emerging best practice and 'lessons learned, identifying and understanding the mechanisms through which emerging practice affects the LAP, how well it is implemented, its strengths and any barriers and challenges faced from an action research perspective incorporating the 'lived experiences' of the partnerships involved in Children in and out of prison.

LAP Data transfer:

Child Referral to LAP Service: The referring Youth Offending Service will complete the referral which consist of child's risk assessments and criminal convictions and sends this information to

	the Youth Offending Service SPOC's (from each local authority in that sub region) and the appointed LAP Provider via Secure Email. The Youth Offending SPOC's then complete their own background checks and risk assessment and transfers this information back to the referring Youth Offending Service. This information is discussed as part of a sub regional LAP multi-agency meeting with the SPOC's and appointed LAP provider to endorse the referral or not. The LAP appointed provider will store the child's screening, referral form, risk assessments etc.. on a secure system, likely to be their existing child safeguarding case management system. As with normal safeguarding processes, data on a child or family who cross borough boundaries will be shared between those councils. **During Placement:** The team around the child will meet with the child and placement information and intervention plans are shared between the local authority and provider via secure email (CJSM) on a monthly basis. Referrals to the commissioned organisations will be completed by the Youth Offending Services and St Christophers Fellowship to allow the receiving organisations to complete their own risk and safeguarding assessments. **After Placement:** up to 12 months following the child leaving the placement their re-offending, convictions etc.. will be tracked with the relevant local authorities and external evaluator to support with evaluation of the LAP project. Information will be shared via secure email. Data may also be shared regarding children's peers or associates who are not themselves referred to the LAP through the processes above where this is necessary and proportionate for safeguarding purposes. **Why is this being done:** Sharing data on the children at the LAP will enable us to gain a greater understanding of the complexities, prevalence and impact of children on intensive support packages in the community across the Pathfinder area. This will help us to better target local resources, respond effectively to local need and identify emerging good practice for wider implementation. To properly safeguard children, victims, and the public in a residential context where risks of harm have the potential to be high.

	We also need to measure the impact of the project, which will include child and service outcomes which will be facilitated by an external evaluator.		
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. 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 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 Offending 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 project is subject to the Working Together to Safeguard Children/Information Sharing Guidance referred to above. The multi-agency referral and decision making process mitigates the risk of inaccurate data analysis by a single individual or agency. 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 MACE meetings (or equivalents). 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?** *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 at the LAP.		
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?** *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?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*		

	Consent is not the lawful basis for sharing. However, in practical terms agreement of the person is needed as every child placed at the LAP will have agreed to be placed there, including the agreement of their parents/carers. This agreement will be included as part of the court proceedings. Essentially, every child would agree to be placed in the care of the local authority via a section 20 Children's Act 1989.	
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** *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 their secure case management systems LA drives/folders St Christophers Fellowship: Will keep sensitive data on secure network systems or secure filling cabinets/lockers at each of the accommodations . Camden Local Authority: As the lead local authority Camden will keep sensitive case level data on a secure network drive via share point which is restricted. Middlesex University: Will have selected staff having access to specific sensitive case level data via Camden restricted shared point folder. Commissioned Organisations under the Pathfinder: Will store data on their own secure systems and network drives.	
4.11	**Data Retention Period** *How long will the data be kept?*	
	St Christopher will retain the data for 12 years after the expiry of the contract. Local authorities have their own retention schedules and these will apply as necessary. 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.	
4.12		Yes/No

	Will this information be shared/processed outside the organisations listed above in question 3? *If yes, describe who and why:*	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)	

- Local Authorities' nominated SPOCs
- St Christophers Fellowship management team
- Middlesex University evaluation project team
- Wipers Youth CIC selected management team
- Fight for Peace Academy selected management team
- Fitness Education Programme selected management team
- Street Doctors selected management team

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		Yes/No

	Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below: SLSP is required for new systems. *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.*	No
5.6	**Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?** *Please explain and give reference to such plan and protocol*	Yes/No 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?	
	The LAP Strategic Development Manager will run the reports but this will not make reference to personal data	
	• What roles will receive the report or where will it be published?	
	London Accommodation Resettlement Partnership Board which has a wide multi agency representation that has strategic oversight of the project.	
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?	
	Pseudonymised and Anonymised	
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
	Business sensitive	

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** 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; Personal data could be obtained and misused by malicious parties within the organisation. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Possible	Major	12- Medium/High
Misuse of data (fair, lawful and transparent); 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. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Possible	Major	12 - Medium/high
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; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Possible	Major	12 - Medium/High Risk
Further transfer of data; 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	Unlikely	Moderate	6- Moderate Risk

safeguards. Staff users send personal data insecurely outside UK due to lack of physical controls in place Compliance risk; Personal data shall be obtained for one or more specified and lawful purposes. Appropriate technical and organisational measures shall be taken. Personal data shall not be transferred outside the European Economic Area. Corporate risk; Reputational risk. Loss of trust			
Data accuracy Inaccurate data collected: Data corrupted or metadata altered by users. Users forget they have shared files or Files shared/deleted incorrectly Corporate risk; Reputational risk. Loss of trust. Legal implications	Unlikely	Major	8 -Moderate Risk
Unauthorised access of data: 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.. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications	Possible	Major	12- Medium/High
Data Retention: Risks that appointed provider will retain data beyond a defined period given in their contract. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications	Unlikely	Minor	8- Medium/High risk
Data subject rights: 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	• Appointed Provider policy and procedures to cover this • Appointed provider staff training around data protection and GDPR • 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. • Ensure only secure email is used to process the data and password protected documents where required • Ensure that LAP multi agency across local authorities are clear about their expectations and that this is written into the LAP operations manual that each LA will have. • Clear emphasis in the evaluators spec that no personal information should be used and everything is anonymised and they will be held to a contract • Evaluation report will be signed off at the board before being allowed to be published	Reduced	9 - Medium	Yes
Theft of Data	• 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.	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. • 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 Offending Services and shared in a safe and secure way to subregional groups and appointed provider. • Data process is set out in data flow chart. • No data can be downloaded by councils who have read only access • This will be monitored by the LAP strategic manager to ensure all services are being compliant	Reduced	6 - Moderate	Yes
Unauthorised access of data:	• Clear protocol • Staff training around IT security, • Locking of workstations, security of paper records. • Ongoing management vigilance to ensure protocols are followed. • Audit/Spot checks at accommodation sites	Reduced	6- Moderate	Yes
Data Retention:	• Any data recorded eg nominal status in council records will be subject to council retention periods. • Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. • This Record of Processing Activity (ROPA) must include the retention period for the data. • All partners must a destruction of records policy in place. Information must not be retained for longer than necessary for the purpose for which it was obtained. • Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.	Reduced	6-Moderate	Yes

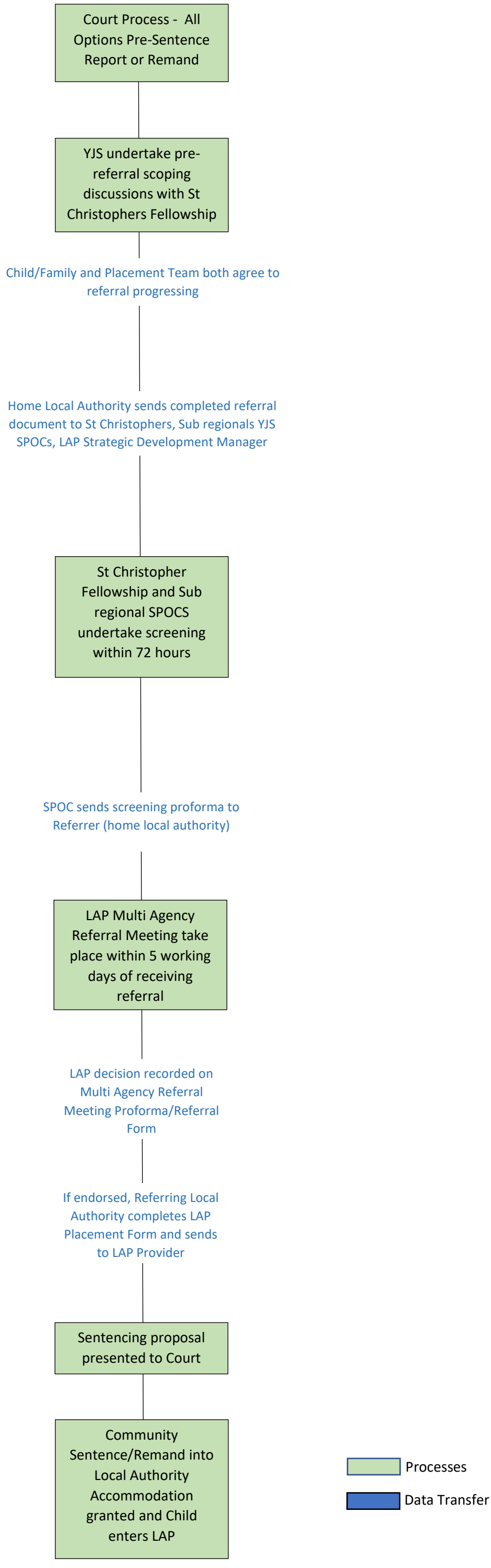
	• Retention and disposal will be written in Provider and external evaluators contract			

Overall residual risk level: Medium

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		
Residual risks approved by:		
DPO advice provided:	Sarah Laws, October 2022	
Summary of DPO advice for each council (Note that local DPOs for each organisation need to produce their own DPIAs, or consciously adopt this suggested DPIA). I am content with this processing Andrew Maughan DPO 27th September 2021 Reviewed following updates October 2022 and re-approved by Andrew Maughan, DPO, 13th October 2022		
This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA

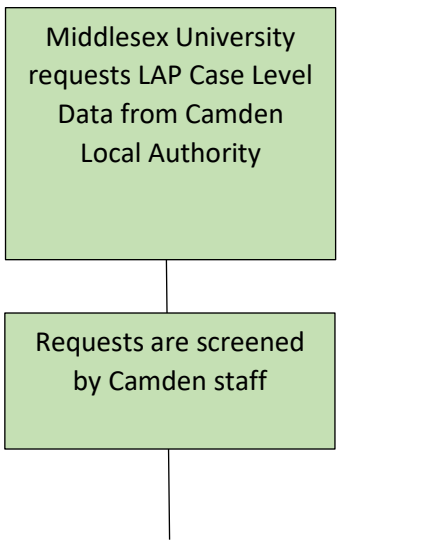
London Accommodation Pathfinder
Data Exchange between Referring Local Authority and LAP Key Stakeholders

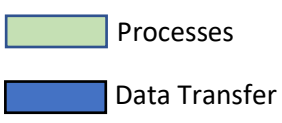
Transfer of Data Flowchart



London Accommodation Pathfinder
Data transfer for External Evaluator
Middlesex University

Transfer of Data Flowchart





London Accommodation Pathfinder
Data Exchange between Camden Council and Participating Local Authorities

Transfer of Data Flowchart

