Data Protection Impact Assessment

Version	Reason	Date	Author(s)
1.0	New	21/06/2023	Joe Luxton
1.1	Reviewed and approved by Islington IG Panel	29/06/2023	Joe Luxton

Project / Work Stream Name	LIIA Project: SEND Insights	
Project / Work Stream Lead	Name	Joe Luxton
	Designation	Data Protection Manager – London Borough of Islington
	Telephone	020 7527 8002
	Email	Joe.luxton@islington.gov.uk
Overview: (Summary of the project/work stream)	**Overview and context** London has a regional approach to sector-led improvement, overseen by the Association of London Directors of Children's Services (ALDCS). Known as the 'London Innovation and Improvement Alliance (LIIA), this is a standing body for cooperating on the improvement of Children's Services through identification and sharing of best practice, including creation of shared datasets and comparative analyses. Within the LIIA structure we have a shared analytical team, currently based at London Councils, and with IT based at LB Waltham Forest. They agree questions to be answered with the ALDCS and deliver it by taking in aggregate data from all Boroughs, producing pan-London analyses, and sharing these back to the ALDCS. As the LIIA has matured, the DSCs have begun to ask for analysis of issues which are important to improving outcomes in London, but which require boroughs to share personal data. Therefore, they have commissioned this project to establish a secure and ethical approach to conducting any pan-London analyses which rely on individual-level data.	

The process is being designed around three principles:

- **Respect for the rights of data subjects** – data processing is proportionate to benefits, and in line with subjects' expectations about how that data should be used.
- **Minimising work for Boroughs** – by using wherever possible datasets which each borough already has and relying on the pan-London infrastructure already created for data collaborations including IGfL, the London DataStore, and the Information Sharing Gateway.
- **Focus on use cases which improve outcomes** – enabling us to maximise improvement for the resources spent, and clearly link each act of processing to a specific legitimate purpose

The LIIA team are being supported in this by Social Finance, a not-for-profit data specialist who have previously developed the information governance and technical infrastructure for multi-LA data collaborations using individual-level data from children's services data.

Following on from the Children's Services Insights project and responding to the requests from the DCS' relating to the LIIA/ ALDCS SEND priority, we would like to extend the CLD data to include the SEN2 return which has become a child-level statutory return for the first time in 2023.

Benefits, Necessity, and Proportionality

We wish to:

- Improve developmental, safeguarding, and wellbeing outcomes for children and young people with Special Educational Needs – by providing analysis which helps DCSs and their teams to identify and prioritize opportunities for improvement and identify good practice in other broughs from which they could learn.
- Address disproportionality by identifying the extent to which minoritized groups have different trajectories – children and young people who might be over/under served by SEND services and are more or less likely to benefit from the support being provided.

We believe that these benefits are clearly sufficient to justify the processing if it is necessary and proportionate.

Necessity

An example of the type of analysis DCSs are demanding from Children's Services data, at the intersection of these two public tasks, is useful here.

> *DCSs are mindful that, given systemic racism, it is likely that SEND work will be under and over scrutinising different ethnic groups. With reference to research carried out by Steve Strand and Ariel Lindorff, 'Ethnic disproportionality in the identification of Special Educational Needs (SEN) in England' (2018), analysis will allow DCSs to examine if the identified disproportionality is present in the London SEN system and within their individual LA*
>
> *They are attracted to the 'Relative Rate Index' approach proposed for justice in the Lammy Review.*
>
> *Plainly – there's a good chance that BAME families in London are over-scrutinised by local authorities and their partners and those responsible for the system need to be able to see this in order to address it.*

Additionally, Regional London analysis on special educational needs will give DCSs and other LA stakeholders insights into:

- Rates of special educational needs across London by factors such as gender, ethnicity, IMD and SEN characteristics – identified need, phase, educational establishment
- Identification of groups of children for whom there appears to be a disproportionate system response, using relative rate indices and other forms of visualisation
- Data on the system responsiveness to children who may have special educational needs
- Links to other vulnerabilities where a different part of the children services system may be providing a service

Put together, these insights provide DCSs and special education leads in LAs with the information to support targeted interventions to improve the outcomes of children with special needs in their Boroughs.

The project team cannot serve the DCSs analytical requirement using aggregate data already available to it. We came to the conclusion that the types of analyses they want to commission clearly service the public tasks, and that we cannot deliver the analysis using aggregate data.

Contractual Arrangements

The LIIA team have already developed a common Data Processing Agreement (DPA) and contract to be used between each Data Controller, and the Data Processor. DPAs have also been agreed between the Data Processor (London Councils) and all sub-processors involved in processing. These agreements developed in consultation with the Information Governance Group for London (IGfL).

Here we are adding the SEN2 Use case to the existing Use Cases using the same ‘LIIA CLD’ approach to collecting the data from the 33 London local authorities and processing it to produces SEND insights (described below).

The ‘once for London’ approach championed by the LIIA Project means establishing a single platform to manage the secure processing and distribution of data for multiple use cases. It also recommends a ‘once for London’ approach to Information Governance, with a main agreement for the project purpose, and additions to this agreement for each use case.

Each use case is subject to individual approval by the ALDCS, and will be subject to:

- a separate Schedule in the DPA between London Councils and the Boroughs
- it’s own DPO’s guide for a DPIA.,

The first time that DPOs scrutinised this project, they gave their approval for:

- the main project purpose
- data processing common across all use cases
- the use cases known at the launch of the project

The agreement made was that when new use cases (such as this one) are agreed by ALDCS and proposed for development, DPOs from all London Boroughs will be asked to review and approve new additions to the agreement, in the form of a new Schedule and a new DPIA guide

This DPIA supports the use case: **SEND Insights**, and corresponds to Schedule 6 of the DPA between LIIA and the Boroughs.

Overview of Intended Processing: Common to all use cases

- Each Borough uploads data, including personal sensitive data, onto a private, borough-specific folder in the London Datastore.

- Scripts provided by the LIIA team then processes this data on the London DataStore in three ways:
    1. Preparation of single Borough’s data for analysis, including:
        - i. Checking whether agreed pseudonymisation and data minimisation has been done prior to sending, and implementing it if not (e.g. deletion of fields not required; degrading highly disclosive data such as postcodes and dates of birth);
        - ii. Assessment of data quality (missing values, logically inconsistent values);
        - iii. Transformation of data to conform to a common schema.
    2. Loading the prepared data for all Boroughs into a pan-London database;
    3. Creating extracts from that database for analytical purposes specific to the use case.
- The single-Borough output of step 1 are made available back to the Borough, free for them to use for their own internal analysis
- The extracts created in step 3 are made available to an approved analyst (either at London Councils or a named sub-processor approved by the DPOs) to produce the pan-London analyses specific to the use case
-

<u>Use case: SEND Insights</u>

Context

This use case for the LIIA Project involves aggregating and sharing Boroughs’ data from the SEN2 return produced as part of Boroughs’ statutory duties. The analysis, to be conducted by LIIA analysts at London Borough of Waltham Forest (LBWF), aims to:

- Allow Directors of Children’s Services (DCSs) to be aware of the current state of the special educational system in London.
- With reference to research carried out by Steve Strand and Ariel Lindorff, ‘Ethnic disproportionality in the identification of Special Educational Needs (SEN) in England’ (2018), allow DCSs to examine if the identified disproportionality is present in the London SEN system and within their individual LA .
- Allow more detailed analysis of distribution of children with identified special educational needs and the prevalence of their access to SEN services across London relative to factors including LA of residence, sex, ethnicity, age, deprivation.

	● Allow DCSs to examine the relationship between their SEN, Children’s social care and education cohorts and explore the potential for improving service delivery and efficiency. ● Support the work of ALDCS (Association of London Directors of Children’s Services) on the SEND priority, which is one of the key ALDCS/ LIIA (London Innovation & Improvement Alliance) priorities Data will be aggregated and shared such that no individuals are identifiable. Information will be analysed at the Borough level, with Boroughs identified in the shared analysis. The analysis will be shared only among DCSs, senior managers and data professionals in London local authorities. **Use Case Specific Data Processing** • Pan-London extracts for SEN2 accessed by LIIA analysts at LBWF via a secure bearer token to Power BI hosted by LBWF • Individual-level data are held in cache in Power BI, accessible only by LIIA analysts at LBWF • Descriptive analysis of event frequencies and breakdown by Borough, age group, ethnicity group, with comparison by Borough conducted in Power BI report • Power BI report shared with DCSs, senior managers and data professionals through personal, secure link. Data in report can be accessed at Borough-level only
Implementation Date:	Estimated by August 2023
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. *Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or refereed articles published by industry associations, technology providers, and research centres.*	**Why We Think This May Need a DPIA** The data to be processed concerns vulnerable individuals (e.g. children and families in contact with children’s services). Data will be anonymised to the fullest extent possible, but in most cases it will retain some risk of identification by third parties in the event of a data breach. The purposes are analysis of administrative data for the purpose of delivering the LAs’ statutory duties - with an explicit bar on: identification of individual data subjects, determining whether individuals do or do not get a service, automating any decision making about an individual, use of machine learning. These purposes and means are not novel and are in line with the Boroughs’ existing privacy notices. In addition, two things that might have been considered novel, have already been carried out through the CLD project:

	1. Sending their data to a third party (LBWF) to be processed instead of doing it in-house (although we note that the same data is routinely provided to the third parties DfE and to Ofsted to for similar processing and purpose); 2. Combining their data with that of other Boroughs to enable new questions to be answered (although we note that both DfE and Ofsted are known to combine the same datasets and conduct similar processing for the same purpose). The same data is already transferred to third parties (DfE and Ofsted) and combined with data from other LAs in order to conduct very similar processing for a very similar purpose, this is not novel processing. However, there is sufficient ambiguity about whether that removes novelty to warrant consideration of a DPIA. Given the ‘once for London’ approach central to the LIIA project, and the standardisation of processes and data flows that is established, we believe it is legitimate for a full DPIA to be conducted by only one Borough, on behalf of all others, and that summary DPIAs are sufficient for all others.

Step 1: Complete the Screening Questions

Q	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?	Yes
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?	Yes
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?	Yes (Potentially)
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
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
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?	Yes
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No

Q	Category	Screening question	Yes/No
1.12	Exemptions and Exceptions	Does the project’s justification include significant contributions to public security and measures?	No
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
		Changed

2.2	What data will be processed/shared/viewed?									
	Personal Data									
	Forename		Surname		Date of Birth	X	Age	X	Gender	X
	Address		Postal address		Employment records		Email address		Postcode	X
	Other unique identifier (*please specify*) UPN - Unique Pupil Number ULN – Unique Learner Number URN – Unique Reference No.		Telephone number		Driving license number		NHS No		Hospital ID no	
	Other data *(Please state):*			**Data Subjects** **Children and Young People** who meet any of the following conditions: • the subject of a request for an assessment for an Education, Health & Care Plan (EHCP) • the subject of an EHC assessment • the subject of an EHCP at any time • the subject of mediation or a tribunal under the SEND code of conduct						

Practically, this is intended to include children and young people included in the SEN2 annual statutory return

What Data

The data being used is pseudonymised administrative data collected in the delivery of services, for the purposes of statutory reporting and the purposes noted above.

The definitive list of fields is attached as Appendix 2 – 'The Data Extracts and Their Scope'. In summary, it covers:

- Unique identifiers (e.g. unique pupil number)
- Demographics (e.g. gender, age, ethnicity)
- Requests and assessments (e.g. dates, outcomes)
- Reviews (e.g. dates and outcomes of reviews)
- Education Health and Care Plans (e.g. start, end, need code)
- Mediations and Tribunals (dates)

Inclusion of Personal Data

Yes – for at least some subjects data will cover:

- Gender - required for equalities monitoring
- Location based data (degraded postcode identifying clusters of c. 3,000 households, collected for children in care placements) - required to understand links between area characteristics (e.g. inferred socio-economic status; gang territories) and needs/outcomes, to answer questions such as whether some areas might be under/over-served, and whether children placed 'out of area' have worse outcomes

Other Unique Identifiers – unique pupil number and per-LA child ID are captured to assist with checking data quality, and re-linking data across Cin Census, the SSDA903, and Annex A.

Special Categories of Personal Data					
Racial or ethnic origin	X	Political opinion		Religious or philosophical beliefs	
Trade Union membership		Physical or mental health or condition			X
Sexual life or sexual orientation		Social service records		Child protection records	

	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							
	Other data *(Please state):*	Yes – for at least some data subjects, the data includes: • Racial or ethnic origin – required for equalities monitoring Mental and physical health (via a 'SEND need code' applied following assessment') – required to understand needs and to identify good practice in meeting them						
	Will the dataset include clinical data? (please include)	No						
	Will the dataset include financial data?	No						
	Description of other data processed/shared/viewed?							

2.3	Business sensitive data	Y/N	Details
	Financial	No	N/A
	Local Contract conditions	No	N/A
	Operational data	No	N/A
	Notes associated with patentable inventions	No	N/A
	procurement/tendering information	No	N/A
	Customer/supplier information	No	N/A
	Decisions impacting:	One or more business function	Y/N No
		Across the organisation	No
	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*		Yes/No
			Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or [Data Security and Protection (DSP) Toolkit]
			Yes / No
	Local Authorities (Signatories to the Child Level DPA for London boroughs)	Controller	Yes (generally)
	London Councils	Processor	TBC
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. This will be covered in the Child Level DPA for London Boroughs
3.3	Has a data flow mapping exercise been undertaken? If yes, please provide a copy at Annex 2 below, if no, please undertake one		See attached Data Flow map in Appendix 1
3.4	Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?		Yes / No
			No

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)*
	Sharing SEND Insights The project exists to help the London Directors of Children's Services to deliver their statutory obligations under section 17 of the Children's Act 1989 "to safeguard and promote the welfare of children in need in their area" and section 149 of the Equality Act 2010 to deliver the "public sector equality duty". It aims to do this by: a. **Accelerating service improvement** – by enabling the identification and prioritisation of opportunities for improvement, and the identification of good practice in other boroughs;

	b. **Monitoring equalities** – by enabling comparative analysis of the odds of key SEND interventions being used with families of different ethnicities. Through this, the project aims to benefit vulnerable children, young people, and their families by improving the quality of services which provide necessary support for their special educational needs to help them to develop to their full potential.

Step 4: Assess necessity and proportionality			
4.1	Lawfulness for Processing/sharing personal data/special categories of personal data?		
	UK GDPR	DPA 2018	Other Lawful Basis
	Personally Identifiable Data		
	UK GDPR Article 6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	The DPA section 8(c) – "the exercise of a function conferred on a person by an enactment or rule of law", specifically the public tasks are: • "to safeguard and promote the welfare of children within their area who are in need" – a statutory duty under the Children's Act 1989 • To deliver the "public sector equality duty" outlined in the Equalities Act 2010 including the needs to "advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it" and to "take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it" • This is reinforced in the SEN Code of Conduct "Public bodies, including further	

			education institutions, local authorities, maintained schools, maintained nursery schools, academies and free schools are covered by the public sector equality duty and, when carrying out their functions, must have regard to the need to eliminate discrimination, promote equality of opportunity and foster good relations between disabled and nondisabled children and young people.” • The SEND Code of Conduct also places a responsiobility on all partners that they should be; “Using information to understand and predict need for services 3.27 To inform commissioning decisions, partners should draw on the wide range of local data sets as well as qualitative information about the likely education, health and social care needs of children and young people with SEN or disabilities.” • And in relation to improve service offered it says; “Local authorities must review the special educational provision and social care provision in their areas for children and young people who have SEN or disabilities and the provision made for local children and young people who are educated out of the area, working with the partners to their joint commissioning arrangements.”		

Special Categories of Personally Identifiable Data		
UK GDPR Article 9(2)(g) '…processing is necessary for reasons of substantial public interest…'	The DPA Schedule 1 Part 2 section 2 "'Safeguarding of children and individuals at risk' and 'Equality of opportunity or treatment' satisfying DPA section 10 (3)	

4.2	Will the information be processed/shared electronically, on paper or both?	Electronic	X
		Paper	
4.3	How will you ensure data quality and data minimisation?		

Data Quality

- Each Borough uploads data, including personal sensitive data, onto a private, borough-specific folder in the London Datastore.
- Scripts provided by the LIIA team then processes this data on the London DataStore in three ways:
    4. Preparation of single Borough's data for analysis, including:
        i. Checking whether agreed pseudonymisation and data minimisation has been done prior to sending, and implementing it if not (e.g. deletion of fields not required; degrading highly disclosive data such as postcodes and dates of birth);
        ii. Assessment of data quality (missing values, logically inconsistent values);
        iii. Transformation of data to conform to a common schema.
    5. Loading the prepared data for all Boroughs into a pan-London database;
    6. Creating extracts from that database for analytical purposes specific to the use case.
- The single-Borough output of step 1 are made available back to the Borough, free for them to use for their own internal analysis
- The extracts created in step 3 are made available to an approved analyst (either at London Councils or a named sub-processor approved by the DPOs) to produce the pan-London analyses specific to the use case

Data Minimisation

In this, we are balancing the desire for *data minimisation* with the practical need not to have to ask the LAs for new data extracts each time we specify a question. This is a legitimate trade-off to consider - ICO guidance explaining the application of the Data Protection Act 2018 is clear that *"You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it."*

Our approach is to request a single annual data submission from each LA – making working with the project viable for them in terms of workload, but to then:

1. **Apply minimisation in our specification of the data request**– removing all data which we do not believe we are likely to need for our purposes, and degrading data which is more specific than we need it to be. The precise data request we are making – including which datasets, fields, and periods, is attached as Appendix 2.

   Specifically:

   a. Removing a large number of individuals from our scope by:

      i. restricting the analysis to individuals who are in scope during a twelve-year period – (see retention and deletion pages 5 & 6 in this document).

   b. Removing data fields from our scope where we are unlikely to require them for the types of analyses which serve our purposes – e.g. name (if we have UPN or ULN for matching across years)

2. **Protect anonymity** – Degrading indirect identifiers which have a greater level of specificity than we believe we are likely to need – e.g. postcode to postcode sector (a c. 200x reduction in specificity) and date of birth to month of birth and school year (a c. 30x reduction in specificity).

3. **Incorporate Minimisation into our ETL Process** – essentially setting the code which prepares the data ready for use to check that minimisation has been applied by the sender, and then to apply it automatically if it has not – deleting and degrading data as appropriate before it is loaded into the database for analysis.

Controlling Function Creep

A key risk here is that having authorised processing for one purpose, the unit then begins to stretch and eventually break the agreed scope.

To control this:

- All lines of enquiry will need to be agreed with by the ALDCS through their regular meeting, or by their nominated representative (currently Ben Byrne, Strategic Lead for the London innovation and Improvement Alliance);
- Local Authority DPOs will have the option to subscribe to a regular update letting them know what lines of enquiry are being pursued and how they relate to the purpose, and we will maintain regular contact with IGfL to allow them to scrutinise the work.
- A summary of each enquiry (although not the outputs) will be publicly logged on the LIIA website, with the purpose it relates to.

All new use cases, that change the nature of the data being shared and/or the purpose of its processing will be subject to additional approvals from DPOs through the additions of new Schedules to the DPA between London Councils and London Boroughs and the creation of new guides for DPIAs, such as this one

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 patients on their websites?*	Yes/No TBC
	Participating boroughs will need to review their fair processing notices as per the guidance in Appendix 3	
4.5	How will you help to support the rights of individuals?	
	Processor obligations are addressed in para.7 of the DSA	
4.6	Are arrangements in place for recognising and responding to Subject Access Requests (SARs)? *If no, please describe how rights are exercised. If Yes, please detail.*	Yes/No Yes
	Each Local Authority (Controller) will be responsible for managing Subject Access Request through their internal corporate procedures. Processor responsibilities to assist with Data Subject Rights requests is addressed in para.7 of the DSA	
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*	Yes/No No
No. There are prior concerns about the use of machine learning and automated decision making in Children's Services, and so these have been placed out of scope. This scope restriction will be written into the DPAs between data controllers and the data processor.		
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.*	Yes/No No
	Relying on other lawful basis	
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 cloud security questionnaire and add as an annex or state below why it is not required.	Yes/No Yes
	See 4.10	
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.*	
	Where Data is Stored and Processed	

	Data will be stored and processed on a secure environment within the new SDS platform; subject to technical, physical, and process controls as befits the sensitivity of the data. Data is hosted on Amazon Web services in either the Dublin or Frankfurt data centres, as the London AWS centre does not offer the right features; the European Commission adequacy decision recognized UK data protection laws as equivalent with EU laws, enabling data to flow freely between the UK and the EU. The AWS data centre is secure and highly monitored (full list of procedures in place available here). AWS is certified ISO 27001 (full list of AWS certifications available here). Several safeguards are in place to ensure resilience of the data storage, leading to the repellence of previous denial-of-service (DoS) attacks. These include annual penetration tests. Data protection from loss and lack of availability on AWS is covered by their business continuity and disaster recovery policy. Connections to the SDS platform will be encrypted and authenticated using the same methods used to secure and encrypt sensitive information like credit cards, usernames, passwords and other private data sent over the internet. Uploads to the SDS platform are Private as default and access is possible only through individual user accounts with secure passwords. IGfL colleagues are involved in the SDS development project to ensue the SDS platform will be comparable with secure '.gov.uk' email accounts. We consider this platform will be an appropriate solution for storing and processing data from all London Boroughs, with the choice to pseudonymise and minimise data from the source datasets to be conducted here, rather than at each Borough. This will ensure that standardised datasets are received and will minimise the data processing requirements of each Borough, in line with our 'once for London' approach.
4.11	Data Retention Period *How long will the data be kept?*
	The original intention had been to store data going back up to six years from the point of analysis. Previous analysis finds that six years is the minimum for good quality journey analysis (an analytical approach we expect to employ), but that having more than six years' data does not materially help to answer new questions or answer existing questions with greater certainty or granularity. However, we have subsequently found that this creates a barrier to properly understanding the journeys of children through the Children's Services system and that the journeys of many of the children receiving children's services in London are truncated by this approach We therefore propose to extend the period covered to eleven years to cover the journey from birth to the beginning of adolescence or the beginning of adolescence to the transition to leaving care (and all the variations in between and then review if that is sufficient. We will build on the existing data from 2016/17 and add subsequent years data as they become available to accumulate to eleven years' worth of data.

	The DPA places a duty on the processor (and any sub-processors) to securely destroy any data outside this scope (e.g. if over time we come to have twelve years' data) and to destroy all data at the end of the programme or on request of the data controller, unless at the point of review it is felt that there is a robust and proportionate case for extending further. The intention is not to extend indefinitely and certainly not beyond 25 years – which would cover the current statutory responsibilities for Children's Services for both Care Leavers and children with Special Educational Needs – and therefore allow the complete arc of a child's interactions with children's services in these areas to be seen. This would enable service design, practice and resource planning to benefit from the insights gained. The processor is also obliged to evidence this destruction to the controller if requested.	
4.12	Will this information being shared/processed outside the organisations listed above in question 3? If yes, describe who and why:	Yes/No Yes
	Data Source The data is initially collected by frontline staff working for or on behalf of Children's Services as part of the exercise of the authority's statutory duties. It is initially stored in the authority's case management system. Extracts from the application database are then prepared for annually submission to the DfE. These extracts are re-used as inputs for the LIIA pan-London analysis. The processing to produce these pan-London datasets is designed to produce an additional layer of minimisation between the full datasets provided by each Borough, and the data being analysed. Field-level detail of the minimisation that will be conducted is provided in Annex 1. **Where Data is Stored and Processed** Pan-London extracts are accessed by secure extract to Power BI from the London Data Platform by LIIA analysts at LBWF. The extract is a download of the full dataset through a bearer token. Data is stored in cache in Power BI, hosted by LBWF. Analysis to aggregate individual level data to Borough level is conducted in Power BI. Only LIIA analysts working on the project will have access to individual-level data. **Nature of Processing** Descriptive analysis to identify patterns in needs and outcomes, which can support London LAs in planning and improving Children's Services. Outputs will be tables and charts showing aggregate data (no PII) which can be safely shared with the London DCSs. There will be no machine learning, no automated decision making, and no attempts to support decision making about an individual case.	

Step 5: Information Security Process		
5.1	Is there an ability to audit access to the information? *If no, please provide a reason why this is not required. If yes, please describe auditing.*	Yes/No TBC
5.2	How will access to information be controlled?	
	Folder access rights on London Data Platform Access to any part of the platform requires individual access credentials (controlled through the platform identity and access management system and governed by appropriate security technologies i.e. single-sign on via major identity providers, password complexity and multi-factor authentication). Controller's private folder - The CONTROLLER's private folder on the London Data Platform is created manually by the London Data Platform admin. Several staff members from the CONTROLLER can be given access to the folder. The PROCESSOR will not be able to access the data hosted in the CONTROLLER's private folder. Beyond staff at the CONTROLLER, only London Data Platform admin will be able to access this data to grant access rights and initiate data processing. LIIA Analysis folder - The LIIA Analysis folder on the London Data Platform is only accessible by authorised personnel from the PROCESSOR conducting the analysis and the London Data Platform admin and data engineer.	
5.3	What roles will have access to the information? (list individuals or staff groups)	
	Access to Analysis Power BI analysis collected in Power BI report, at a Borough level, with Boroughs identifiable. The report is shared via individual link to named individuals at all London Boroughs. Access to the report is managed by LIIA analysts at LBWF. Links shared with individuals will allow access only to that individual. **Additional Sub-Processors** Social Finance Ltd, a not-for-profit data and strategy specialist is support the LIIA Data & insight team in the production of Python code to prepare the data for analysis. This code is QAd and tested by LIIA Data & insight team and Social Finance. Social Finance are also training the LIIA team, to maintain and extend that code.	
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		Smartcard		key to locked filing cabinet/room	

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

5.5	Is there a documented System Level Security Policy (SLSP) for this project? If yes, please add a copy as an annex. 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.*	Yes/No
		TBC
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
		Yes
	Several safeguards are in place to ensure resilience of the data storage, leading to the repellence of previous denial-of-service (DoS) attacks. These include annual penetration tests. Data protection from loss and lack of availability on AWS is covered by their business continuity and disaster recovery policy.	

5.7	Is Mandatory Staff Training in place for the following?	Yes/No	Dates
	• Data Collection:	London Data Platform staff with access to the systems are all accredited under the ONS Secure Researcher training. LIIA to confirm re: sub processors.	
	• Use of the System or Service:		
	• Information Governance:		

5.8	Are there any new or additional reporting requirements for this project? *If no, skip to 5.9. If yes, provide details below.*	Yes/No
		No
	• What roles will be able to run reports?	
	LIIA analysts at LBWF.	
	• What roles will receive the report or where will it be published?	
	Power BI analysis collected in Power BI report, at a Borough level, with Boroughs identifiable. The report is shared via individual link to named individuals at all London Boroughs. Access to the report is managed by LIIA analysts at LBWF. Links shared with individuals will allow access only to that individual.	

	- Will the reports be in person-identifiable, pseudonymised or anonymised format?	
	Anonymised	
	- Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
	N/A	
5.9	Have any Information Governance risks been identified relating to this project? If yes, the final section must 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
Data Breach	High	Low	Medium
Data Subjects Unaware of or Not Understanding Processing	Low	High	Medium
Scope Creep takes analysis beyond legitimate purpose	Medium	Medium	Medium
Reduced Trust in Data Controllers if Project is Misconstrued as involving automated decision making or facilitating new level of surveillance of individuals	Medium	Low	Low

Step 7: Identify Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6

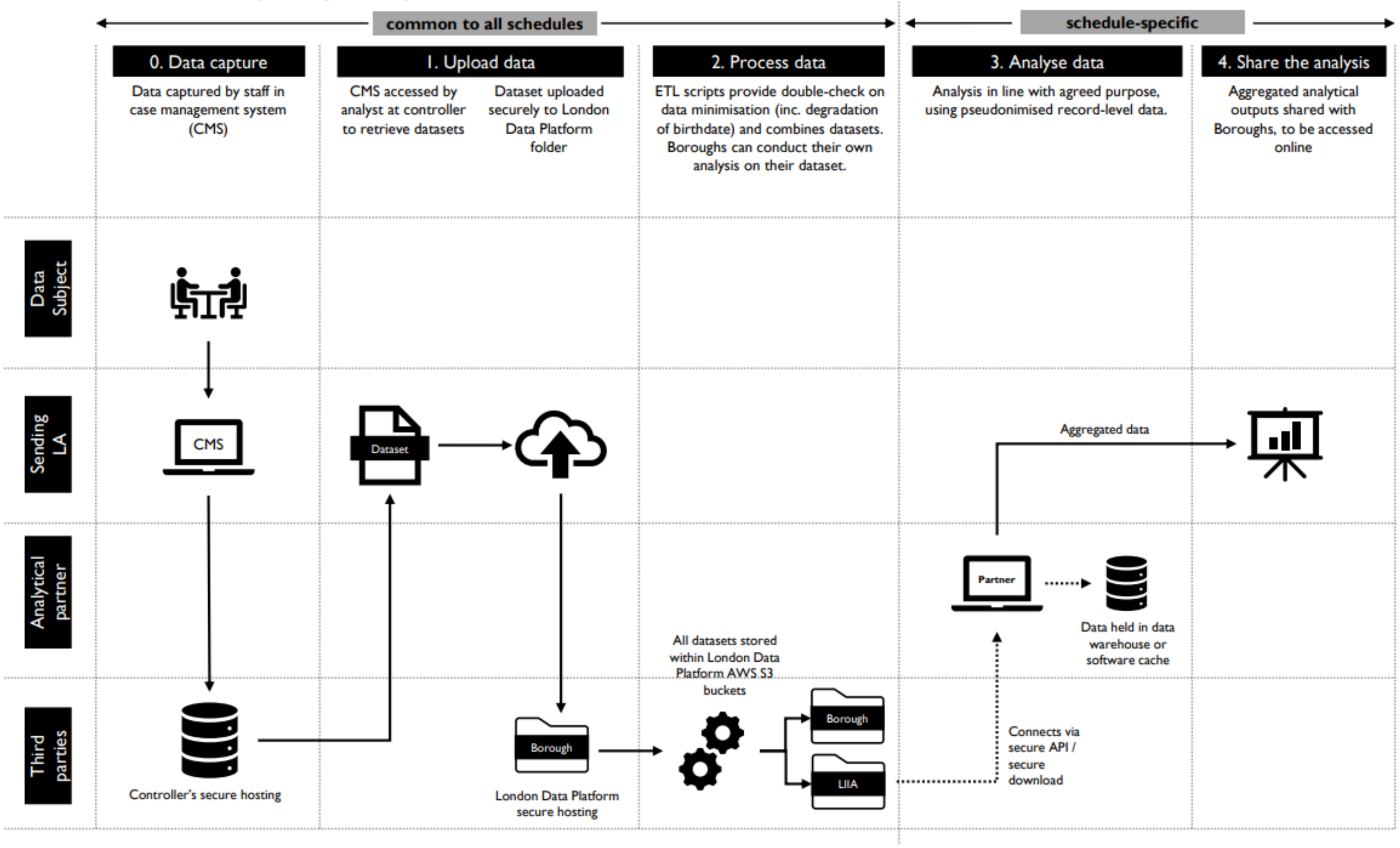
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Data Breach	Data minimisation as outlined above to reduce impact. Technical, physical and process protections legally mandated and auditable – to reduce probability	Reduced	Low-Medium	Yes
Data Subjects Unaware of or Not Understanding Processing	Review privacy notices prior to going live and amend if required Public communication about the project – specifically addressing this.	Reduced	Low	Yes
Scope Creep takes analysis beyond legitimate purpose	Enhanced governance and transparency as outlined above	Reduced	Low	Yes
Reduced Trust in Data Controllers if Project is Misconstrued as involving automated decision making or facilitating new level of surveillance of individuals	Public communication about the project – specifically addressing this. Reduces likelihood that one person misconstruing the purpose spreads.	Reduced	Low	Yes

Step 8: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	Joe Luxton 27/06/2023	
Residual risks approved by:	Joe Luxton 27/06/2023	
DPO advice provided:	Leila Ridley 04/07/2023	
Summary of DPO advice: I am happy to approve this processing – Leila Ridley		
DPO advice accepted or overruled by:	**N/A**	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	**N/A**	If your decision departs from individuals' views, you must explain your reasons
Comments:		
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

Appendix 1: Data Flow

Data Flows – LIIA (v. May 2023)



common to all schedules

schedule-specific

0. Data capture

Data captured by staff in case management system (CMS)

1. Upload data

CMS accessed by analyst at controller to retrieve datasets

Dataset uploaded securely to London Data Platform folder

2. Process data

ETL scripts provide double-check on data minimisation (inc. degradation of birthdate) and combines datasets. Boroughs can conduct their own analysis on their dataset.

3. Analyse data

Analysis in line with agreed purpose, using pseudonimised record-level data.

4. Share the analysis

Aggregated analytical outputs shared with Boroughs, to be accessed online

Data Subject
Sending LA
Analytical partner
Third parties
CMS
Dataset
Controller's secure hosting
Borough
London Data Platform secure hosting
All datasets stored within London Data Platform AWS S3 buckets
Borough
LIIA
Connects via secure API / secure download
Partner
Data held in data warehouse or software cache
Aggregated data

Appendix 2: Data Extracts and their Scope

SEN2 collection data items v2.xlsx

Appendix 3: Note on privacy notices

Most Boroughs will already have privacy notices that provide sufficient information about the processes described here. However, for Boroughs that wish to provide specific information about the project in their Children's Services privacy notice, we recommend the following wording to be added:

London Innovation and Improvement Alliance

The LIIA project is a pan-London initiative to address important issues for children in London that can only be answered by examining London's data as a whole. By creating a secure platform where local authorities can share data with each other and other analysts, the project will improve the breadth and quality of data analysis available to local authorities in London.

Data agreements are in place to ensure that:

- under no circumstances will the data be used for any automated decision making
- all data is transferred, handled or stored in accordance with the Data Protection Act
- access to the data is confined to the smallest possible number of people to produce the analysis
- all data is destroyed after twelve years

You have the right to object to your data being used this way. If you wish to exercise it then please contact *<insert details>*.

Appendix 4: DPO’s guide to Data Protection Impact Assessment (supporting documentation used to complete this DPIA)

LIIA DPO's guide to
DPIA - SEND Children