

NYDPIA69 -3991 -CHI10 - Microsoft knowledge mining pilot - Data Protection Impact Assessment

Organisation Name/Data Controller Name: North Yorkshire Council

Date final DPIA issued 20/03/2024

Data protection impact assessment

Project Brief and Go Live Date – project completion date 31 March 2024.

The aims of the project once complete is to enable Microsoft Azure functionality to run over the top of our existing systems, Liquid Logic (LCS) to allow searching at the push of a button rather than existing manual processes.

Currently information is stored in structured and unstructured ways which can make accessing the right information a time-consuming task. This sometimes leads to us not being able to find the right information or spending hours searching in each different silo.

This technology will also analyse our information in a way that will help us to create ecomaps which will be used to identify networks around children (from information we already hold) and help identify people or places that might protect or pose a risk to children.

The creation of ecomaps is already undertaken by Social Workers as part of their casework, this project is looking at an alternative way of creating these.

The technology will give us the ability to analyse text, audio, photographs including within documents (document cracking through Optical Character Recognition and Entity Recognition) alongside our traditional forms and documents to free up social workers from their computers.

The benefits to the organisation could be significant. We envisage that we will be able to:

- Make better decisions quicker – because we'll have access to the right information quicker.
- Identify networks to protect children, this could reduce the need for statutory services to be overly involved in family life.
- Proactively protect children from risks which up to now we generally come across in hindsight – such as abusive adults having relationships with a succession of vulnerable parents, and their children witnessing domestic abuse incidents for example.
- Free social workers up from spending unproductive time at their computers, with the potential to utilise things like voice notes and voice to text inputs rather than having to sit down and type.
- Proactively protect children from contextual safeguarding risks or risks that are outside of the immediate family.

The DPIA covers the development and pilot workshops of this technology. During the project NYC worked with delivery partners Microsoft and Simpson Associates to develop search and ecomap tools, the project worked with CYPS users to develop and test the tools.

The initial phase was undertaken using a copy of data from LCS, held in the secure Azure Knowledge Mining tenancy, later work looked at developing an incremental refresh to connect live data.

CYPS data is being used to develop and test tools and no decisions about data subjects will be made.

The DPIA was continually updated and amended during each phase of the project.

Project Manager/Owner:

Name:	Jonny Hoyle
Job Title:	Development Lead
Service:	CYPS Children & Families Service
Telephone:	01609532892
Email:	Jonny.hoyle@northyorks.gov.uk
Name:	Claire Wilson

Job Title:	Project Manager
Service:	Strategic Resources
Telephone:	01609 532802
Email:	Claire.wilson@northyorks.gov.uk

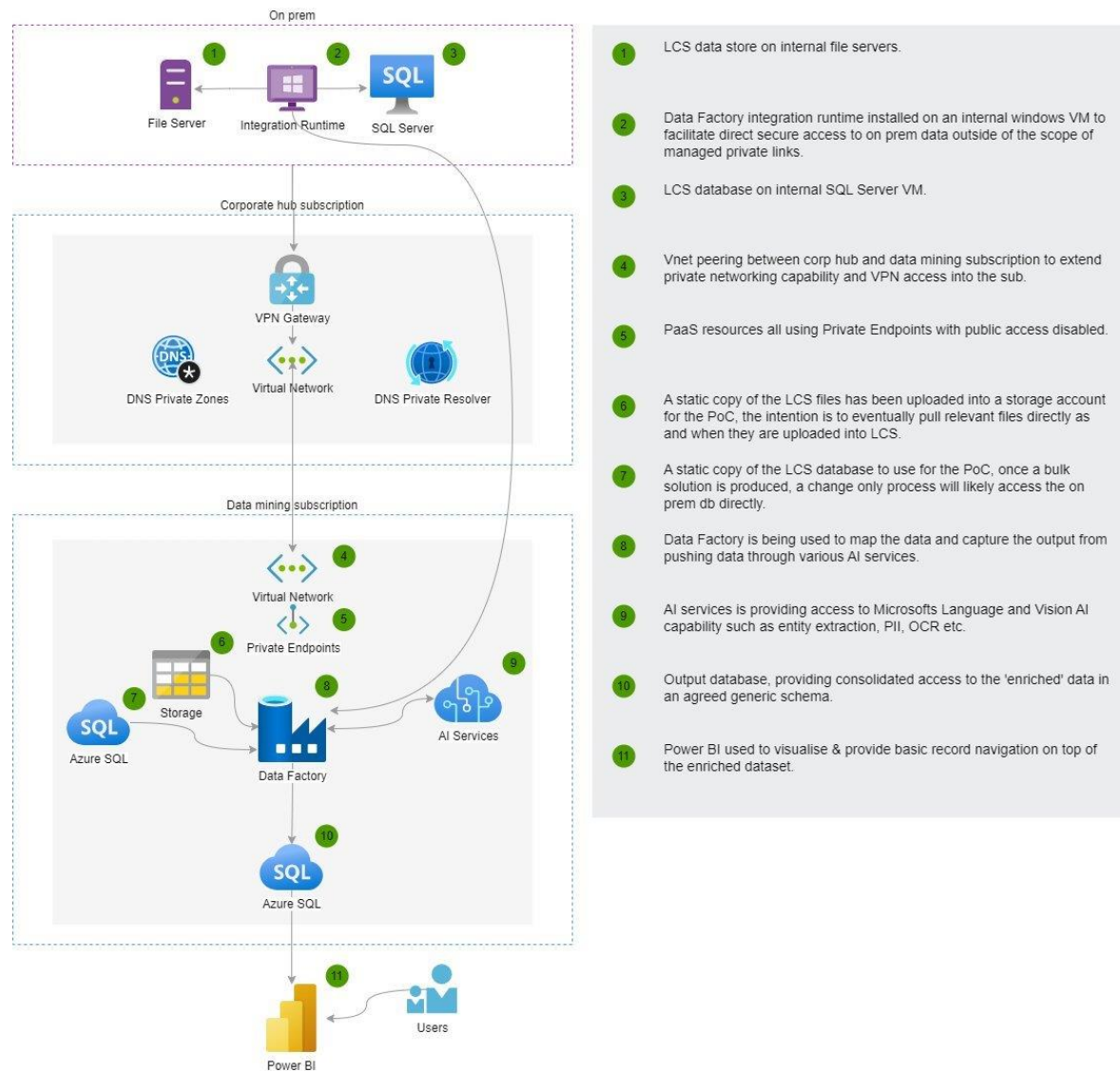
Information Asset Owner/s:

Name:	Mel Hutchinson
Job Title:	Assistant Director
Service:	CYPS Children & Families Service
Telephone:	01609 536542
Email:	Mel.hutchinson@northyorks.gov.uk

System Administrator/ICT Contact (if applicable):

Name:	Mark Peterson
Job Title:	Acting Head of Data and Intelligence
Service:	Data and Intelligence
Telephone:	01609 797039
Email:	mark.peterson@northyorks.gov.uk

PART ONE – INFORMATION FLOW



1. LCS data store on internal file servers.
2. Data Factory integration runtime installed on an internal windows VM to facilitate direct secure access to on prem data outside of the scope of managed private links.
3. LCS database on internal SQL Server VM.
4. Vnet peering between corp hub and data mining subscription to extend private networking capability and VPN access into the sub.
5. PaaS resources all using Private Endpoints with public access disabled.
6. A static copy of the LCS files has been uploaded into a storage account for the PoC, the intention is to eventually pull relevant files directly as and when they are uploaded into LCS.
7. A static copy of the LCS database to use for the PoC, once a bulk solution is produced, a change only process will likely access the on prem db directly.
8. Data Factory is being used to map the data and capture the output from pushing data through various AI services.
9. AI services is providing access to Microsofts Language and Vision AI capability such as entity extraction, PII, OCR etc.
10. Output database, providing consolidated access to the 'enriched' data in an agreed generic schema.
11. Power BI used to visualise & provide basic record navigation on top of the enriched dataset.

Above diagram shows infrastructure and narrative – updated January 2024

PART TWO – PRIVACY RISKS QUESTIONNAIRE

Privacy Issue	Comments	Is there a risk? Address in Part Three
1. General		
Have you identified the Information Asset Owner?	Yes	<input type="checkbox"/>
How many individuals will be affected by this project?	<ul style="list-style-type: none"> 456,970 children – this is children (e.g., cases) only, all have unique case reference numbers 1,100,567 significant adults – this is probably more accurately described as a "Child+Adult relationship". If a parent has two children in the system, there will be two significant adult records for that person. One for Parent->Child A, another for Parent->Child B. 331,539 case workers – this works similar to the relationship above, except this is for "Child+Worker relationship". This record also has start and end dates, so 	<input checked="" type="checkbox"/>

	<p>contains a history of those relationships. If a case worker has been assigned a role working with the child over three time periods, there will be three records in for that Child+Worker combination.</p> <p>The dataset will also include other people connected to a child/family through references in casenotes etc.</p>	
Who are the Data Subjects?	<p>All those whose information is stored on our LCS system.</p> <p>The views of CYPS practitioners will be sought as part of the development of the tools and the evaluation of the pilot. This will be undertaken through feedback provided at workshops (feedback will not be attributed to any particular staff member so will be anonymous), and through the use of internal surveys (Microsoft Forms via Business Change). Surveys will not collect names and therefore results will be anonymous.</p>	<input type="checkbox"/>
	Personal Identifiers/information	Special Category / Criminal
		<input checked="" type="checkbox"/>

Please select any information that will be processed:	<input checked="" type="checkbox"/>	Name	<input checked="" type="checkbox"/>	Sex life	
	<input checked="" type="checkbox"/>	Address/Postcode	<input checked="" type="checkbox"/>	Sexual Orientation	
	<input checked="" type="checkbox"/>	Date of Birth	<input checked="" type="checkbox"/>	Religion	
	<input checked="" type="checkbox"/>	Telephone Number/Email	<input checked="" type="checkbox"/>	Philosophical belief	
	<input checked="" type="checkbox"/>	Emergency contact details	<input checked="" type="checkbox"/>	Political opinion	
	<input checked="" type="checkbox"/>	National Insurance Number	<input type="checkbox"/>	Trade Union Membership	
	<input checked="" type="checkbox"/>	NHS Number	<input checked="" type="checkbox"/>	Ethnic Origin	
	<input checked="" type="checkbox"/>	Gender	<input checked="" type="checkbox"/>	Medical history details	
	<input checked="" type="checkbox"/>	Images (photo/film)	<input checked="" type="checkbox"/>	Physical health information	
	<input checked="" type="checkbox"/>	Pseudonymised information	<input checked="" type="checkbox"/>	Mental health information	
	<input type="checkbox"/>	IP addresses	<input type="checkbox"/>	Genetic/Biometric (eg. Thumbprint)	
		<input type="checkbox"/> Other (please state) Could also include the following: Aliases (could be birth name, maiden name, preferred name) UPN (unique pupil number) Child Trust Number Nationality Family members/relationships Marital Status	<input checked="" type="checkbox"/>	Criminal conviction information	
How will the personal data be collected?	Other (please state)				<input type="checkbox"/>
	Other: the information is already on our LCS and EHM systems				
Does this processing include data matching, automated	No automated decision making takes place. No data matching takes place.				<input checked="" type="checkbox"/>

decision making or profiling? (please describe)	No automated profiling takes place.	
2. Lawfulness		
a. General Processing		
What is the lawful basis for processing personal information? If you are using more than one condition please specify which condition relates to specific data. (Please speak with your DPO about this)	e) Public Task (specify) Choose an item. UK GDPR Article 6(1) (e) - The processing of personal information is necessary for the Council to perform a task in the public interest, and the task or function has a clear basis in law.	<input type="checkbox"/>
If you are processing Special Category Information (highlighted in red above), what is the lawful basis for processing this information (Please speak with your DPO about this)	Choose an item. h) Health or social care (check condition 2 in guidance) Schedule 1, Part 1 of the Data Protection Act 2018 as below: (f) the management of health care systems or services or social care systems or services.	<input type="checkbox"/>
	Health & Social Care – data processed for the health and care support that subject may need. Comply with the requirements of Articles 9 and 10 of the UK GDPR, as well as the DPA 2018	
	Yes	<input type="checkbox"/>

Are you processing Criminal conviction information? (Please speak with your DPO about this)	Schedule 1, Part 1 of the Data Protection Act 2018 as below: (18) Safeguarding of children and of individuals at risk		
b. Law Enforcement Processing			
Are you processing data for a Law Enforcement Purpose?	<input type="checkbox"/>	Yes, please specify the legislation that provides the authority to engage in the specific Law Enforcement purpose:	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	No	
If you are processing Special Category Information (highlighted in red above), is it strictly necessary and what condition are you relying on? (Please speak with your DPO about this)	Please state why the special category of information is <u>strictly</u> necessary for the law enforcement purposes: n/a		<input type="checkbox"/>
	Please specify the Schedule condition: n/a		
c. Fairness and Transparency			
If you are using consent, how are you collecting this and how will people be able to withdraw their consent?	Not processed under consent in terms of lawfulness categories.		<input type="checkbox"/>

How will you tell people about this processing?	Privacy notice – it is reasonable for data subjects to expect that the Council processes this information using various systems and processes and that these may be reviewed and updated. https://www.northyorks.gov.uk/your-council/transparency-freedom-information-and-data-protection/privacy-notices/cyps-general-privacy-notice		<input type="checkbox"/>
Do you need to update your privacy notices?		Yes	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	No	
3. Purpose Limitation			
Are you going to use information you already hold about individuals for a purpose it is not currently used for?	<input type="checkbox"/>	Yes, please specify why it is currently held and under which lawful basis:	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	No – the data exists, and the searching/analysis could be undertaken manually.	
Have you identified all of the purposes for which you will use personal information?	<input checked="" type="checkbox"/>	Yes	<input type="checkbox"/>
	<input type="checkbox"/>	No. If no, why not?	
Will people expect their information to be processed in this way?	<input checked="" type="checkbox"/>	Yes	<input type="checkbox"/>
	<input type="checkbox"/>	No, please give details:	
4. Data Minimisation			
How will you ensure you are only collecting information that is relevant to this specific purpose?	The data is already captured on existing systems, there is no data input method available in the tool.		<input type="checkbox"/>

Have you considered what information you could disregard without compromising the project?	<input checked="" type="checkbox"/>	Yes, please detail if any has been removed: None – to be considered as products are developed.	<input type="checkbox"/>
	<input type="checkbox"/>	No	
5. Accuracy			
How are you going to ensure that the personal information will be kept accurate and up to date?	This already happens in the current process during each contact with the client – this project will be reading that data rather than creating its own.		<input type="checkbox"/>
How are you going to ensure that the quality of the data you collect is sufficient for your intended purpose?	This already happens in the current process during each contact with the client – this project will be reading that data rather than creating its own.		<input type="checkbox"/>
If you are procuring a new system, does it allow you to amend and / or delete information when necessary? (Consult IT as necessary)	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	<input type="checkbox"/>	No, please give details:	
	<input type="checkbox"/>	Notes can be added to the system where accuracy is disputed	
	<input checked="" type="checkbox"/>	N/A	
6. Storage Limitation / Records Management			
How long will the information be kept for? (Retention period)	Retention period may differ depending on dataset – this project will not change any existing retention periods. Data will be removed in line with the NYC data retention policy.		<input type="checkbox"/>

	<p>It is anticipated that all changes in the source system would be carried over to this product (including data deleted from source system is not available in the tool). Further is work required to understand this fully.</p> <p>Responsibility for this data is split across CYPS, NYC Technology and NYC Data and Intelligence. Recommendation is that an information asset owner for the product is defined and the information asset register is updated.</p>		
Are you procuring a system that will allow you to delete information in line with your retention periods? (Consult IT as necessary)	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	<input type="checkbox"/>	No, if no why not?	
	<input checked="" type="checkbox"/>	N/A	
What method will be used, to securely destroy paper and/or electronic records? (Consult IT/processor as necessary)	To be considered as tools and associated practice guidance is developed		<input type="checkbox"/>
Will destruction be certificated or added to a destruction log?	<input type="checkbox"/>	Yes, please specify:	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	No, standard NYC practice and procedures.	
Where will information be stored/accessed?	Cloud based applications – Stored in Azure knowledge mining tenancy (for the pilot workshops user access is through a power BI dashboard)		<input type="checkbox"/>
	Other (specify):		
If you are using a 'Cloud Based' system to store or transfer information, where is the	UK South		<input checked="" type="checkbox"/>

geographical location of the server/s? (you may need to ask your provider to supply this)	The provisioned resources are in the UK South datacentre to ensure data is not held outside of the UK.	
If back up information is stored off-site, where is the geographical location?	Back-up is locally redundant to UK South (not geo-redundant)	<input checked="" type="checkbox"/>
7. Security		
Who will have access to the information within the organisation?	<p>Note that social worker teams (or individuals) who will pilot the products are all authorised LCS users have access to the data currently.</p> <p>During the development – limited members of the project team, board, and user experience team (two colleagues) will unavoidably access information during development, evaluation and moderated user experience testing and expert review of prototype. This was discussed and agreed with Data Governance.</p>	<input checked="" type="checkbox"/>
What controls have been put in place to limit access to the information?	<p>Access to sensitive data only when unavoidable, data is not copied, exported or saved locally (unless absolutely necessary).</p> <p>Usual agreements to only access information necessary to carry out work, and asked to declare if there is a personal connection to a child/family on the system.</p> <p>Only one Member of the Simpson team will have access to the data. Password protected remote access to NYC Azure tenancy (Knowledge mining) through Privileged Identity Management (contact is Gordon Aitkin). See info in part 3 risk evaluation.</p>	<input type="checkbox"/>

	geraint.edwards@simpson-associates.co.uk – (only person accessing) Robust vetting process and practice guidance is embedded in CYPs – appropriate viewing of records – only certain people can access the designated systems now, the same cohort would be able to use the tools which search existing records and data. The technical and practice (cultural) impacts of the new tool in terms of access to restricted records is being monitored as project risks.		
If you are implementing a new system, does this system have the ability to audit access (audit trails)?	<input checked="" type="checkbox"/>	Yes The following audit information is available: <ul style="list-style-type: none"> • When the data in a report was updated • Who has accessed the tool, date and time Currently, not able to audit the specifics of what is searched for once within the product, i.e. which individual(s). In terms of options for controlling access from a security perspective, there are several: <ul style="list-style-type: none"> • User access is limited on an account-based approach • Different views (audiences) can be made available to different users, so people only see the pages they need • Could blanketly block or implement row level security to prevent access to restricted records 	<input type="checkbox"/>
	<input type="checkbox"/>	No	

	<input type="checkbox"/>	N/A	
Does your new system/hardware/procedure provide adequate protection against security risks? Please detail. (Consult IT as necessary)		<p>Microsoft and NYC access and safety controls in place. Secure infrastructure has been built by NYC Unified Communications & Security team.</p> <p>Consultation with Microsoft and their delivery partners has been completed, and this project has an industry standard approach to moving sensitive information between on premise systems and Azure.</p> <p>Microsoft submitted to SCOPE Europe the Azure attestation of adherence to the EU Cloud CoC. In doing so, Microsoft relied on independent third-party audits that produce well-established certifications, which are foundational to Azure security and compliance:</p> <ul style="list-style-type: none"> • ISO/IEC 27001 – Information Security Management System • ISO/IEC 27701 – Privacy Information Management System • ISO/IEC 27018 – Cloud Privacy <p>An independent review by SCOPE Europe has demonstrated that Azure meets the EU Cloud CoC second level of compliance.</p>	<input type="checkbox"/>
Are staff undertaking any additional training to help use new systems/procedures? Will this include Data Protection training?	<input checked="" type="checkbox"/>	<p>Yes (please give details)</p> <p>Practice guidance has been developed (which references/signposting to data protection), this will be used alongside internal presentations. The information included in the practice guidance:</p> <p>"Accessing Records</p>	<input type="checkbox"/>

		<p>Do not attempt to access any NYC systems, computer or network unless you are an authorised user. Attempting to access a system to which you have no authorised right of access is a criminal offence under the Computer Misuse Act 1990. Remember Data Protection is a legal requirement.</p> <p>Only access records that you need to look at in connection with your professional role. Inappropriate access is a data breach for which you will be held personally liable, both by NCC, and the ICO.</p> <p>You must not access records of people you know and are not working with professionally. Remember, ALL access is monitored, recorded and audited. Inappropriate access is a data breach.</p> <p>Data protection training for NYC staff is mandatory.</p>	
	<input type="checkbox"/>	No. If no why not?	
Is there a disaster recovery plan in place in case of equipment/software failure? (you may need to ask your provider to supply this)		Yes	<input type="checkbox"/>
		No – this is not applicable for the pilot	
8.Data Processors – Data Processors should be listed after part 2 of this form			
If you are using a data processor, how has the provider demonstrated an adequate level of information	<p>Microsoft is committed to helping protect the security of Customer Data. The security measures Microsoft takes are described in detail in the Product Terms.</p> <p>Microsoft complies with strict security standards and industry-leading</p>		<input type="checkbox"/>

<p>security? (you may need to ask your provider to supply this)</p>	<p>data protection methodology. Microsoft is continually improving its systems to deal with new threats. More information regarding cloud governance and privacy practices is available at Trust Center's Cloud Governance & Privacy page.</p> <p>Microsoft takes reasonable and appropriate technical and organizational measures to safeguard the personal data that it processes. These measures include, but are not limited to, internal privacy policies and practices, contractual commitments, and international and regional standard certifications. More information is available at Trust Center's Privacy Standards page.</p> <p>Microsoft provides significant, transparent customer-facing security and privacy materials to help explain Microsoft's use and processing of personal data. Customers are encouraged to contact Microsoft with questions.</p> <p>Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.</p> <p>Where Microsoft processes personal data for its legitimate business operations, it complies with GDPR obligations that apply to data controllers.</p>	
<p>If using a data processor, how has the provider demonstrated that they are compliant with UK GDPR? (you may need to ask your provider to supply this)</p>	<p>Microsoft have a data processing addendum which contains all the mandatory UK GDPR clauses. It appears that this applies to Azure. There has been no negotiation with Microsoft regarding these clauses.</p> <p>Microsoft will retain and process Customer Data during the Customer's right to use the Online Service and until all Customer Data is retrieved by Customer or deleted in accordance with the terms of the Product Terms and Products and Services Data Protection Addendum (DPA). During the term of Customer's subscription, the Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so</p>	<p>☒</p>

	<p>that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data. The customer can delete personal data pursuant to a Data Subject Request using the capabilities described in the Azure Data Subject Request GDPR Documentation.</p> <p>General Data Protection Regulation GDPR Overview (microsoft.com)</p> <p>General Data Protection Regulation - Microsoft GDPR Microsoft Docs</p> <p>Simpson Associates acted as a data processor, included in risk evaluation (mitigations all took place). One member of staff from Simpson Associates who assisted delivery, covered by NYC/Simpsons contract including data protection agreement signed January 2024.</p> <p>All external access is password protected and via secure Privileged Identity Management.</p>		
If using a data processor, do you have a written contract in place with UK GDPR clauses?	<input checked="" type="checkbox"/>	Yes – NYC/Microsoft corporate agreement NYC/ Simpson Associates contract	<input type="checkbox"/>
	<input type="checkbox"/>	No	
	<input type="checkbox"/>	N/A	
9. Information Sharing – Data Controllers should be listed after part 2 of this form			
What is the legal basis for sharing?	Contract		<input type="checkbox"/>

Is there a sharing agreement in place?	<input checked="" type="checkbox"/>	Yes (please attach)	<input type="checkbox"/>
	<input type="checkbox"/>	No. If no, why not?	
	<input type="checkbox"/>	N/A	
Will you transfer information outside of the UK, where will this be?	<input type="checkbox"/>	Yes, please specify where:	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	No – UK South	
		N/A	
How will information be transferred?	Best practice data security is in place – see diagram in 'Information Flow' section (page 4).		<input type="checkbox"/>
10. Rights of the Data Subject			
How will you manage 'Subject Access Requests' or other requests regarding information rights? (Rectification, erasure, objection, and restriction etc.)	These will continue with the current NYC process		<input type="checkbox"/>
If procuring a new system, will this allow you to fulfil the rights of the data subject mentioned above?		Yes, detail as needed:	<input type="checkbox"/>
		No – not applicable	
If the project involves automated decision making do you have a process in place to facilitate human intervention? Please detail.	No automated decision making.		<input type="checkbox"/>

Will your data processing exclude individuals from using a service or from exercising any rights?	<input type="checkbox"/>	Yes, detail as needed:	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	No	
11. Accountability			
As a result of this project do you need to update any of the following?	<input checked="" type="checkbox"/>	Information Asset Register (Information Asset Owner for product would need to be added to IAR when rolled out to services)	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	Policies – required when rolled out to services	
	<input checked="" type="checkbox"/>	Procedures – required when rolled out to services	
If needed, have you consulted relevant stakeholders/Caldicott Guardian/ICO? What was the outcome?		<p>Yes, who? please add outcome details:</p> <p>There is a project Board in place and external governance through DfE Data & Digital Solutions Fund Programme.</p> <p>The project is piloting the council's AI ethics impact assessment.</p> <p>CYPS senior leadership and workforce involved in Locality events Nov/Dec 2023 and at pilot workshops.</p>	<input type="checkbox"/>
		No	

List any Data Controllers information will be shared with (if applicable):

Name:	
Contact Details:	

Name:	
Contact Details:	
Name:	
Contact Details:	
Name:	
Contact Details:	

List any Data Processors information will be processed by (if applicable):

Name:	Jaz Arora - Microsoft
Contact Details:	jaznique.arora@microsoft.com
Name:	Geraint Edwards - Simpson's Associates
Contact Details:	Geraint.edwards@simpson-associates.co.uk
Name:	
Contact Details:	
Name:	
Contact Details:	

PART THREE – RISK EVALUATION

Privacy Risks (from part two) Describe source of risk and potential impact on individuals, compliance and corporate risks (as needed)	Impact (harm to individual) minimal, some or serious X Likelihood remote, possible or probable = Risk	Options to reduce or eliminate risk	Overall Risk after options implemented Impact (harm to individual) minimal, some or serious X Likelihood remote, possible or probable = Risk	Evaluation eliminated, reduced, accepted
Large number of data subjects	Low Risk	All individual's data processed in the same way. Transferred digitally so no human error. Secure transfers	Low Risk	Accept Data Gov and Project Board
Special category data being processed – no anonymity	Medium Risk	Secure transfers of data into cloud Transferred digitally so no human error.	Low Risk	Accept Data Gov and Project Board
Data subjects are not aware of how their data is being processed, resulting in complaints or escalation to ICO	Low Risk	Council privacy notices informs data subjects. The data exists and the searching/analysis could be undertaken manually. It is reasonable for data subjects to expect that the Council processes this information using various systems and processes and that these may be reviewed and updated.	Low Risk	Accept Data Gov and Project Board
Information asset register is not up to date	Medium Risk	Determine who the Information Asset Owner is for the product and update the Information Asset Register	Low Risk	Accept Data Gov
Additional outputs created without sufficient controls over access	Low Risk	No one without relevant permissions/access could create or view output. To continue monitoring as product develops further – to take a view about exporting any outputs if implemented.	Low Risk	Accept Data Gov and Project Board

Simpson Associates are acting as a processor on behalf of Microsoft	Low Risk	<p>Microsoft have a data processing addendum in place stating Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met. However this is part of Caveated terms and conditions therefore no negation has taken place.</p> <p>Update 14/09 – counter to information above MS/Simpsons signed statement of works dated 11 Sept 2023 clarifies Simpsons are not sub-processors. Data gov and DPO confirmed project activities can proceed due to low risk and look to get a data processor agreement in place with Simpson's retrospectively.</p>	Low Risk	Accept (Project Board 31/08)
Simpson Associates have access to a special category data through the data copy.	High Risk	<p>Microsoft standard NDA is in place and covers Simpson Associates.</p> <p>Simpson Associates confirmed they would not store or copy any NYC data outside of the NYC network.</p> <p>Only named Simpson's employees will have access. This is password protected remote access to NYC Azure tenancy (Knowledge mining) through Privileged Identity Management.</p> <p>Wording from NYC devices (below) will be shared with those who have access reminding them of their obligations under UK GDPR and warning about accessing information without business need. <i>(shared by email 31/08 –see below)</i></p> <p>Accessing Records</p> <p>Do not attempt to access any NYC systems, computer or network unless you are an authorised user. Attempting to access a system to which you have no authorised right of access is a criminal offence under the Computer Misuse Act 1990. Remember Data Protection is a legal requirement.</p> <p>Only access records that you need to look at in connection with your professional role. Inappropriate access is a data breach for which you will be held personally liable, both by NYC, and the ICO.</p> <p>You must not access records of people you know and are not working with professionally. Remember, ALL access is monitored, recorded and audited. Inappropriate access is a data breach.</p> <p>Do not copy and paste data into any other system or document.</p>	Low Risk	Accept (Project Board 31/08)

17/11/2023 – Data governance considerations about gathering user feedback and testing at in-person CYPs Locality events Nov/Dec 2023	Low Risk	<p>Locality events background/considerations:</p> <ul style="list-style-type: none"> - 50-100 people at each event, all from CYPs held in private venues (Romanby, Wykeham, Selby and Harrogate, 27 Nov – 5 Dec 2023) - It is reasonable and necessary to do this work with service users to test and refine the solution as part of the proof of concept - Ensured that any record we used to demo is not one that is restricted to anyone <p>Agreed mitigations:</p> <ul style="list-style-type: none"> - Demonstrate that all people attending have business access to that data - Managing the environment – e.g., signs, no entry, re-enforce confidentiality - Particular appropriate record(s) would be used, these could be different for each event - Ask if anyone knows the individual to declare it - Summary of agreed approach: we need to use the live data to make this a useful exercise, appreciate everyone has access, ask if anyone has a declaration of interest and ensure the environment is private 	Low Risk	Accept (Data Governance, David Kempen)
New agreement (NYC / Simpson Associates) for additional work	Low Risk	<ul style="list-style-type: none"> - Produced a standalone additional DPIA which referenced this DPIA - This stated the work being done and referenced the standard data processing agreement from legal (included with the contract) - Same lawful basis etc. some narrative and process (e.g., information flow – OCR and infrastructure) elements were changed 	Low Risk	Accept (Data Gov and Project Board)

Video created for iNetwork awards	Low Risk	<ul style="list-style-type: none"> - Screenshots of product only included anonymised data - Reviewed and approved by Senior Data Governance Officer prior to submission 	Low Risk	Accept (Data Gov and Project Board)
-----------------------------------	----------	---	----------	-------------------------------------

Severity of impact	Serious harm	LowRisk	High Risk	High Risk
	Some impact	LowRisk	Medium Risk	High Risk
	Minimal impact	LowRisk	Low Risk	LowRisk
		Remote	Possible	Probable
		Likelihood of harm		

(Information Commissioners Office, [Risk Matrix](#))

PART FOUR – SIGNATURES AND REVIEW

Information Asset Owner (LiquidLogic)

Name: Mel Hutchinson

Job Title: Assistant Director Children and Families Service

Date: 20/03/2024

Signature:

Data Protection Officer

Name: Naomi Size

Job Title: Information Governance Officer, Veritau

Date: 20/03/2024

Signature: N Size

Data Governance Officer

Name: David Kempen

Job Title: Senior Data Governance Officer

Date: 20/03/2024

Signature: D Kempen

Senior Officer

Name: Mark Peterson

Job Title: Acting Head of Data and Intelligence

Date: 20/03/2024

Signature:

Date of last review: 20/03/2024

NEXT REVIEW DATE: 20/04/2024