DATA PROTECTION IMPACT ASSESSMENT [DPIA]

The GDPR introduced a new mandatory requirement for organisations to identify and then assess high risks to the rights and freedoms of individuals associated with any proposals to process personal data, particularly special category personal data. Please refer to the council's Privacy by Design Policy.

Below is set out a template DPIA form which users are expected to save a copy and complete. The form is divided into 3 parts. Part One should be completed first. If necessary Parts Two and Three should then be completed. Each Part contains further guidance and instructions. Part Three is divided into 3 sections

Instructions:

NB: For any DPIA's relating to Adult Social Care/Children's Services and Public Health (ASC/ChS/PH) please contact Jan Boucher, Information Governance/Caldicott Support Manager, at Janice.boucher@rbkc.gov.uk who can support you in this process.

1. Seek advice from the statutory Data Protection Officer [DPO] on whether you need to complete a DPIA.
2. Obtain a copy of the DPIA Form from the DPO website
3. Contact the Information Management Team [IM Team] or DPO to obtain a unique reference number
4. Complete the DPIA Screening Section – Part One
5. If you answer **No** to any of the screening questions, liaise with the IM Team or for ASC/ChS/PH the IG/Caldicott Support Manager to confirm and then arrange for your head of service or project sponsor (whichever is appropriate) to sign this off.
6. Maintain a copy of Part One in your project folder and send a copy to the IM Team for entry onto the DPIA Register so that this can be recorded against your project
7. If you answer **Yes** to any of the screening questions go on to complete Part Two, and then the risk assessment in Part Three.
8. Complete the DPIA form and liaise with the IM Team to agree mitigations and record actions to be taken to reduce any identified risks. This also includes agreeing timescales for either completing mitigation actions and/or keeping the risks under review.
9. Obtain recommendations from the IM Team or the DPO (whichever is appropriate), add these to your form and send to your Head of Service or project sponsor for final sign off as Information Asset Owner (IAO).
10. Attach a copy of your completed Parts 1-3 of the DPIA to your project folder.
11. Send a final copy of your completed DPIA to the IM Team who will maintain a record of it in the council's DPIA Register
12. If you are required to implement or review your mitigations against an agreed timetable, please include these in your DPIA action plan and complete the online Review Actions columns against your registered DPIA
13. All queries about the DPIA should quote the DPIA Unique Reference Number.
14. Details of all relevant council policies and guidance can be found on the DPO and IM Intranet Pages

PART ONE

DATA PROTECTION IMPACT ASSESSMENT [DPIA] - SCREENING QUESTIONS

DPIA Screening Questions to determine if a DPIA is needed. If the answer to any of these questions is yes, users **must** complete Part Two Data Protection Checklist and Part Three Data Protection Risk Assessment. If the answer is No to **all** the questions in this Part, you do not need to undertake the rest of the DPIA. In Part One Use the end column (Description) to provide additional information

DPIA Reference Number:	A499
Project Title	ICPC/Alternative Pathways Evaluation (for internal use)
Process Owner	Helen Bowring
Author (i.e. person completing this DPIA)	Helen Bowring
Date Completed	05/09/2023

	PART ONE: SCREENING				
	Question	Examples	Yes	No	Description (Optional)
1.	Information about individuals will be collected.	Names, contact details	☒	☐	The Local Authority will hold the contact details of the five families (20 C&YP) who consent to participate in the study. (First name, Surname, phone, email, address to post letters). For professionals (12 practitioners and 5 members of partner agencies), in addition to their contact details, their role within the local authority/partner agency will be documented. This information will be shared with Exeter researchers for them to contact families who have consented to participating in the research. Exeter University will collect from the Local Authority data from cases files collected and held by their social care/FGC services with Exeter on three outcomes for families diverted to a safeguarding FGC. These families will have consented to be part of the study, share their contact details and share the below data. Their data will not be anonymised. The 3 outcomes are: - Outcome 1: who was present in the 6-weekly safeguarding meetings following the FGC meeting [if this meeting takes place]; - Outcome 2: step up or step down of family case at 3 months and 6 months post-FGC; - Outcome 3: any updates to the safeguarding plan during the safeguarding meetings. This data will complement the data Exeter have collected directly with the families through interviews and observations, with the families' consent. Exeter University will collect from the Local Authority data routinely collected by their

	PART ONE: SCREENING				
	Question	Examples	Yes	No	Description (Optional)
					social care/FGC services on three key child protection outcomes for two cohorts of families referred to the child protection pathway as described in the study protocol under the routine data collection 2 (social care/FGC service records) (ICPC/FGC pathway). The data will be extracted from LA social care/FGC service records by a designated staff from the LA using a Data Collection Template (pro forma). The data collection template will be shared with the LA in advance. The data will be anonymised prior to being shared with the researcher-in-residence and participant IDs will be used at source: The Data Collection Template will include space for anonymised participant ID, allocated on collection so the data cannot be tracked back to an individual child or family. A single copy of a participant key (linking unique study identifier with case number) will be kept on LA protected SharePoint site and destroyed by the designated staff from LA at end of data collection period to ensure data collected is not identifiable to any specific child, family, or wider network. The extracted and anonymized data will be transferred to a secure encrypted research data storage hub provided by the University of Exeter (RDS) via RiR encrypted laptop. This data consists of: - Cohort 1: all families referred to the child protection pathway in period 12 – 6 months prior to implementation (from 01/04/2022 to 31/03/2023); - Cohort 2: all families referred to the child protection pathway in the period 0 - 3 months post implementation (from 01/04/2023 to 31/12/2023).

	PART ONE: SCREENING				
	Question	Examples	Yes	No	Description (Optional)
					The three key CP outcomes at 6 months post ICPC/FGC for each cohorts are: - CP outcome 1: referred families stepped up and stepped down; - CP outcome 2: referred families with children in care, with family, other community care arrangements; - CP outcome 3: number and spread of family members and professionals attending meetings (FGC/ICPC and all follow-up 6 weekly meetings on CP pathway) [only if this is routinely collected by local authorities]. Exeter University will collect the following information about individuals, families and practitioners from semi-structured interviews, meeting observations and reflection workshops: - In observations (professionals/partners, young people and families), what different people in the meeting say and do. This isn't an assessment of the meeting or participation in it. No personal data or special category data will be captured. (this is not recorded) - In interviews (professionals/partners, young people and families), what their experiences of the Safeguarding FGC are, including what is working well or less well, and how they think the meetings could be improved. No one will be asked about their personal circumstances and sharing special category information is discouraged. (this will be recorded, with consent) - In workshops (professionals/partners, young people and families), what are their experiences of piloting the pathway.

	PART ONE: SCREENING				
	Question	Examples	Yes	No	Description (Optional)
2.	Individuals will be required to provide information about themselves.	Names, contact details	☒	☐	See Part 1, Question 1.
3.	Information about individuals will be disclosed to other organisations or people or transferred outside of the UK. This includes HR and OH data about Council staff.	Social services, debt advice, police, fraud prevention	☐	☒	
4.	Information about individuals will be used for a different purpose than that for which it was originally provided.	Utilising names & addresses for unrelated marketing campaigns		☒	
5.	New technologies, or a new application of existing technologies, will be used.	New technologies might include fingerprint recognition, facial recognition, biometrics etc. New self-service solutions for residents, or development of new database applications using existing customer data	☐	☒	
6.	Automated decisions or actions against individuals with no human intervention will be taken that can have a significant impact on them.	Automatically sending out arrear's letters to tenants in arrears without a manual check.	☐	☒	
7.	Profiling information about individuals will be carried out and used to make decisions on someone's access to a service, opportunity or benefit.	Targeting people based on profiling data such as age, ethnicity or religion for services and goods	☐	☒	

	PART ONE: SCREENING				
	Question	Examples	Yes	No	Description (Optional)
8.	Personal data from multiple sources is combined, compared or matched.	Use of data warehouse for determining fraudulent housing benefit claims	☐	☒	
9.	Personal data is processed without providing a privacy notice directly to the individual.	New data collection form is introduced with no privacy notice or declaration	☐	☒	
10.	Personal data will be processed in a way which involves tracking individuals' online or offline location or behaviour.	Lone worker devices, cookies, google analytics	☐	☒	
11.	Children's personal data will be processed.	Tenancy household composition	☒	☐	young people (over age of 15) can only participate in consultation if they have signed a consent form, any child under 13 will require a parental consent.
12.	CCTV will be used.	Recorded image or video will be captured, which may include identifiable images of people.	☐	☒	
13.	Personal data will be processed which could result in a risk of physical harm in the event of a security breach.	Domestic violence, people flagged as a high risk to staff or other customers.	☐	☒	

Recommendation	
Is a DPIA required?	Yes ☒ No ☐
If No, obtain sign off from the IM Team and place a copy on the project file	
Author (i.e. person completing this DPIA)	
Date Completed	
IMT Sign Off	

PART TWO

PART TWO: **DATA PROTECTION IMPACT CHECKLIST**
Part Two is to be completed if you answered **Yes** to any section of Part One: DPIA Screening. Part Two is intended as a guide to help you identify how your project or initiative will engage the GDPR and Data Protection Act 2018. This will then enable you to complete Part Three (sections 1, 2 and 3) which focus on the risks and issues associated with your proposed processing of personal data. P**lease** complete the Part Two Checklist.

DPIA Reference Number:	
Project Title:	ICPC/Alternative Pathways Evaluation (for internal use)
DPIA Completed By:	Helen Bowring
Project Sponsor:	Amana Gordon
Date DPIA Completed:	05/09/2023

	Question	Guidance	Response
1.	Explain broadly what the project aims to achieve and what type of processing it involves.	*You may find it helpful to refer or link to other documents, such as a project proposal brief or PID.*	Local Authorities are changing the way they work with families by offering people the option to take part in a different type of meeting than previously – called a Family Group Conference. Family Group Conference - a strengths-based, family-led forum - is an alternative way in which Local Authorities can protect children, ensuring parents, children and other family members take part in decision-making and feel more empowered and respected while doing so. Exeter University will speak with family members and friends supporting a family going through this to understand whether the

	Question	Guidance	Response
			choice to have a Family Group Conference might improve family experiences of child protection work. This project research will show how it works best, what outcomes are improved, which families it works for, and in what way. It will also give a better understanding of the perspectives and experiences of families and professionals engaged in the Family Group Conferencing process. The purpose of this evaluation programme is to engage with young people, families and practitioners who have participated in the Alternative Pathway programme to seek their input into shaping and determining outcomes that others can learn from. This is a joint evaluation with LBC and H&F and Bi-Borough and builds on a previous programme and evaluation conducted in 2020. Attached below is the DPIA that is in place for the existing H&F and Bi-Borough ICPC/SFGC Alternative pathway that will inform the evaluation. This was completed in conjunction with Stephen Weaver H&F and Jan Boucher Bi-borough.  Bi Borough DPIA - Final (Jans comments This DPIA sets out the inclusion of H&F and LBC as a participating study site. As a participating site, information will be collected from CP practitioners engaged with the SFGC process in H&F and LBC who attend workshops, meetings with the study team, and participate in semi-structured interviews in order to gain a full assessment of how FGC can be effectively embedded as an alternative pathway to ICPC. As a case study site, H&F and LBC will host a Researcher-in-Residence (RiR). Their presence will help them understand the issues for professional teams working in child protection, as well as to

	Question	Guidance	Response
			make links with families who have opted to join the alternative FGC pathway and who might take part in the study. Social workers will contact families already known to them and ask if they want to participate in the project. If the family agree to be contacted, the researcher will contact them in the way the family tell the social worker they would like the research team to contact them (phone, email, letter, in-person) to discuss what taking part involves and provide a copy of the information sheet and consent form. When relevant and agreed with social workers, potential family participants will be given a short information sheet/contact card by the RiR on first meeting, followed up by a full Information Sheet and Consent Form if interested. Should the researcher be unable to meet the family, the information sheet can be given by the FGC Coordinator when they approach the family. There will be no special interest information given to the research team other than the name and contact details.  WP3_Info_FCS_EFF_V6_15_08_23  WP3_Con_FCS_EFF_V7_20_09_23  WP3_Info_FCS_under12_V4_22_04_04  WP3_Con_FCS_under12_Int_V6_23_07_07  WP3_Info_FCS_12to15_V6_15_08_23  WP3_Con_FCS_12to15_Int_V3_20_09_23

	Question	Guidance	Response
			The Local Authority will hold the contact details of the families who consent to participate in the study. (First name, Surname, phone, email, address to post letters). For professionals (12 practitioners and 5 members of partner agencies), in addition to their contact details, their role within the local authority/partner agency will be documented. This information will be shared with Exeter researchers for them to contact families who have consented to participating in the research.  WP3_Info_FCS_PC_V5_15_08_23  WP3_Con_FCS_PC_Int_V3_20_09_23  WP3_Info_FCS_Prof_V6_15_08_23  WP3_Con_FCS_Prof_V7_20_09_23 Exeter University will collect from the Local Authority data from cases files collected and held by their social care/FGC services with Exeter on three outcomes for families diverted to a safeguarding FGC. This data is collected at three time points [6 weekly review; 3 months post-SFGC; 6 months post-SFGC]. A transparent process of data collection will be instigated with H&F and LBC and agreed in a Data Sharing Agreement. These families will have consented to be part of the study, share their contact details and share the below data. Their data will not be anonymised. The 3 outcomes are: - Outcome 1: who was present in the 6-weekly safeguarding meetings following the FGC meeting [if this meeting takes place]; - Outcome 2: step up or step down of family case at 3 months and 6 months post-FGC; - Outcome 3: any updates to the safeguarding plan during the safeguarding meetings.

	Question	Guidance	Response
			This data will complement the data Exeter will collect directly with the families through interviews and observations, with the families' consent. Exeter University will collect from the Local Authority data routinely collected by their social care/FGC services on three key child protection outcomes for two cohorts of families referred to the child protection pathway as described in the study protocol under the routine data collection 2 (social care/FGC service records) (ICPC/FGC pathway). This data will be anonymised and consists of: - Cohort 1: all families referred to the child protection pathway in period 12 – 6 months prior to implementation (from 01/04/2022 to 31/03/2023); - Cohort 2: all families referred to the child protection pathway in the period 0 - 3 months post implementation (from 01/04/2023 to 31/12/2023). A Data Sharing Agreement will determine how routine data can be extracted from social care/FGC service records in a way that protects participants. All these processes have been approved by our Ethic committee. The three key CP outcomes at 6 months post ICPC/FGC for each cohorts are: - CP outcome 1: referred families stepped up and stepped down; - CP outcome 2: referred families with children in care, with family, other community care arrangements; - CP outcome 3: number and spread of family members and professionals attending meetings (FGC/ICPC and all follow-up 6 weekly meetings on CP pathway) [only if this is routinely collected by local authorities].

	Question	Guidance	Response
			The data will be extracted from LA social care/FGC service records by a designated staff from the LA using a Data Collection Template (pro forma), which includes space for anonymised participant ID. The data will be anonymised prior to being shared with the researcher-in-residence and participant IDs will be used at source, so the data cannot be tracked back to an individual child or family. A single copy of a participant key (linking unique study identifier with case number) will be kept on LA protected SharePoint site and destroyed by the designated staff from LA at end of data collection period to ensure data collected is not identifiable to any specific child, family, or wider network. The extracted data (anonymized and not) will be transferred to a secure encrypted research data storage hub provided by the University of Exeter (RDS). It will be transferred to Exeter either using Egress or encrypted email with the password sent separately to a RiR encrypted laptop. Exeter University will collect the following information about individuals, families and practitioners from semi-structured interviews, meeting observations and reflection workshops: - In observations (professionals/partners, young people, and families), what different people in the meeting say and do. This isn't an assessment of the meeting or participation in it. Notes will be taken at meeting, but anonymised and thematic instead of personal. The meetings will not be recorded. No personal data or special category data will be captured. (this is not recorded) - In interviews (professionals/partners, young people, and families), what their experiences of the Safeguarding FGC are, including what is working well or less well, and how they think the meetings could be improved. No one will be asked about their personal circumstances and sharing special category information is discouraged. In the case of a child, parental consent to participate will be obtained, any interviews with a child will take place in the

	Question	Guidance	Response
			presence of parent who has also signed consent to participate and or relevant practitioner in the case of a young person. (this will be recorded, with consent, transcribed and then made anonymous) - In workshops (professionals/partners, young people, and families), what are their experiences of piloting the pathway. All participants will be allocated a unique study identifying number (ID). A document will link the ID with individuals to ensure that participants are given the same ID across the different data sets. However, once allocated, data will be identifiable only using the participant identifying number. The data collected will be able to be identified by the research team only, and in the case of the participants, they may request to opt out and for their data to be removed up to the point of analysis and write up by using the unique study identifying number (ID) allocated. Audio recordings, transcripts, interviews, routine data, and learning workshop notes will be kept securely, identified by this unique ID and stored separately from the document linking unique IDs to individuals. Measures will be put in place to ensure that participants' identities are not revealed outside the study team. Once audio data has been transcribed, all references to people or place names in the transcripts will be removed. Participants will be informed of our data protection measures prior to data collection. Qualitative data (either in quotes or if-then statements) shared with stakeholders/collaborators/PPI members or in the UK data archive or similar) will be anonymised fully beyond stripping out names, given that the sites and families may have distinctive characteristics which would de-anonymise them to anyone familiar with the limited number of sites where the research study is operating. Once the analysis and the write up are processed, data will

	Question	Guidance	Response
			be embedded in the research and would not be linked to an ID anymore.
2.	Please describe the data that you will be processing. Including whether the data subjects are tenants, service users, Council employees etc.	*List sets of data rather than individual fields, such as customer names, contact information, customer representatives, household members, addresses, profiling data, arrears data, and repairs history.*	Service Users: - Family Contact Details - Social care/FGC services case files on outcomes for families diverted to a safeguarding FGC (not anonymised) - Social care/FGC services records of three key child protection outcomes for two cohorts of families referred to the child protection pathway (anonymised) - Experience with Safeguarding FGC Council Employees: - Practitioner and Partner Agency Contact Details - Practitioner and Partner Agency Role - Practitioner and Partner Agency experience with Safeguarding FGC, including what is working well or less well, and how they think the meetings could be improved.
3.	Is the Council the Data Controller, the Data Processor or a Joint-Controller?		The University of Exeter, H&F, and LBC will act as independent controllers and shall observe all their respective obligations set out in the UK GDPR and the DPA in respect of the Processing of the Personal Data being.
4.	What volume of personal data is being processed?	*How many data subjects (approximately) will be in the dataset being processed?*	12 Practitioners 5 Partners 5 Families 20 C&YP
5.	What is the lawful basis for processing the data? For example, tenancy agreement, lease, contract, specific consent.	*If you do not have a lawful basis then you cannot process the data. You need to seek advice from the IM Team*	No contact details will be shared and no personal data collected by the Local Authority will be made accessible without consent being obtained by the Local Authority from the participants. This will be

	Question	Guidance	Response
		on the lawful basis before proceeding with this project.	informed by an information leaflet setting out the nature of being involved, what information will be shared and what will happen to the information shared. All conversation (interviews) will have an attached consent form that sets out they consent to the anonymised feedback being used. A process will be in place to review an individuals' consent options should they change their mind at any point. However, for the purposes of the UK GDPR, this DPIA does not rely upon explicit consent as its condition for processing. The Councils rely on Article 6.1. (e) Public Task to evaluate families experience of conferences. Article 9 (2) (j) – Archiving and Research, processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The ICPC/Alternative Pathways Evaluation gathers personal data, pseudonymises it and then anonymises the data after analysis for research purposes to help in understanding families' and professionals' journeys with the Safeguarding Family Conference. The anonymised data outputs will be valuable for improving families' experience with child protection work and determining the effectiveness the Family Group Conference process.

	Question	Guidance	Response
6.	Are you using the data in a way that differs from the reason it was originally collected?	*You cannot use the data for a different purpose etc. without reviewing your lawful basis, and steps taken to notify the service users whose data you intend to process.* *If the answer is yes, i.e. you intend to use for a different purpose seek advice from the Council's IM team before proceeding.*	No
7.	Is there another way of achieving the same project outcomes that does not involve processing individuals' data? What other options have you considered?	*This is to ensure that the scope of the project and data processing is in proportion with the expected outcomes.* *Consider whether any data items can be removed, but still achieve the same ends.*	For families, it will be vital to talk to those who have been involved in the Alternative pathway, which would require data sharing of name and contact details.

	Question	Guidance	Response
8.	Does the data / processing include any of the following categories of data? If yes, please indicate which ones and provide a justification for processing the data: • Other household members or named individuals • Named children • Health & medical information including vulnerability • Race and ethnic origin; • Politics and trade union membership • religion; • genetics & biometrics (where used for ID purposes); • health; • sex life or sexual orientation.	*If you collect any of these categories, you must take extra care when processing this data.* *You cannot request data because they may be useful in the future.* *If any apply (you will be processing special category/sensitive personal data) consider adding this as part of your risk assessment.* *Consider whether all the data items specified are required for the processing? Can any be removed, but still achieve the same ends?*	None of the categories apply, all participants will be reminded throughout the conversations/interviews, not to share any personal data about themselves or others. If they do, it will not be noted. In the case where participants are sharing special category information, the audio records are held on a secure encrypted research data storage hub provided by the University of Exeter (RDS). No one except the research team and external transcriber will access the RDS and the researchers and transcriber will have signed a non-disclosure agreement. Once the transcription is returned, the audio record will be deleted. The transcriber is a university supplier who has experience of working with sensitive data, including that of children and young people who may be vulnerable and is subject to a confidential agreement. In the case where participants disclose experience of or potential for harm, the researcher will work to safeguarding policies and procedures in the study settings (Local Authority Children's Services) and to the procedure outlined in the Appendix 8 (Policy for the protection of Participants) of our study protocol – please see below.  Appendix 8 Policy for the Protection of Parti

	Question	Guidance	Response
9.	What is the source of the data?	*Examples include the customer themselves, a representative of the customer, another organisation e.g. NHS partners, voluntary sector etc. Or another WCC/RBKC department.* ***List all that apply.*** *If you are receiving data from a third-party organisation (excluding WCC/RBKC departments) you must be able to explain how you obtained the data and provide copies of any data sharing agreements, contracts or both.*	H&F and LBC Children Social Services. Contact information of the families and professionals will be acquired by H&F and LBC employees who are known to the young person, family member and practitioners. They will seek their consent to engage in the research.
10.	Has a privacy notice been made available to all the data subjects?	*Have data subjects been informed about this new processing, and any third-parties that will have access to their personal data?*	Fair processing notice for children's services can be found at: Children's services privacy notice | LBHF www.camden.gov.uk/privacy
11.	What checks do you have in place to ensure the data will be accurate and kept up to date?	*Reasonable steps must be in place to ensure that data is accurate and kept up to date. Explain how your proposal will maintain accuracy*	Cross referenced with the business analyst who inputs into the data system with Children's Services.
12.	How will you ensure that the data collection process is secure, has an Information Security Questionnaire been completed and reviewed by the Information Security Team?	*Examples of potentially non-secure data collection include, paper forms, unencrypted devices, non-secure email, use of fax machines.*	Researchers have completed the 3rd party assurance ISQ setting out how they will store information. Information will be stored on an encrypted system held by Exeter University as the host. approved copy of 20211231 3rd Party Information Assurance_vFINAL_230322
13.	Who will you be sharing data with, and how will you be sharing the data?	*List all third-party organisations and WCC/RBKC departments.*	H&F and LBC will share data with Exeter University either using Egress or encrypted email with the password sent separately to a RiR encrypted laptop. Data will not be shared outside the UK.

	Question	Guidance	Response
	Will the data ever be moved outside of the UK?	*You must have data sharing agreements in place, if you are sharing with third party organisations (excluding WCC/RBKC departments).* *Examples of data sharing mechanisms include, automated data extracts, data manually uploaded onto an external website, emails to the organisation, posted forms or other documents.* *Consider whether data sharing is compliant and secure as part of your risk assessment.*	Exeter University will share non-anonymised interviews with a transcriber. All information will be anonymised after analysis.
14.	Where will the data be stored and/or processed?	*Please list all relevant systems, business applications, network drives, hosted storage; lockable filing cabinets.* *Please identify exactly where the information will be held on the world wide web. Distinguish between 1) servers and databases hosted entirely on council premises, 2) servers and databases in external or third-party data centres, and 3) cloud-hosted services, servers and databases. If you are not sure, mark this as a risk, and ensure that you find out as part of the procurement process.*	Data will be processed in the UK. The Local Authority, when sharing data, will keep a copy of a participant key (linking unique study identifier with case number) on a protected SharePoint site with designated access and permissions. At the end of the data collection period, these will be destroyed by designated LA staff to ensure it Is not identifiable to any specific child, family, or wider network. Exeter University will store typed notes and audio data on their Research Data Storage (RDS) mapped network drive. Each RDS is unique to a given research project and can only be accessed by users given permissions from the central IT department. RDS security utilises Azure Active Directory (AD) Single Sign-on (SSO). Remote access to RDS is achieved through a Virtual Private Network (VPN) upon which Multi-Factor Authentication (MFA) must be utilised. MFA will comprise of a staff member's username and password, followed by use of the Microsoft Authenticator application on their smartphone.

	Question	Guidance	Response
			All data collection tools and technology used on site (audio recorders and laptops) by the RiR will be encrypted. Identifiable information (consent forms, participant attendance sheets etc.) will be kept on the university's secured SharePoint, separate from data, to ensure that data, after anonymisation, cannot be linked to any individuals. Hard copies of documents such as the consent forms and attendance sheets will be scanned, stored on the secure SharePoint, and disposed of in confidential waste bins. Audio data will be transferred to the professional transcriber, and transcripts returned, by accessing a dedicated folder held on RDS. Transcriber's personal PC has McAfee LiveSafe virus protection, as well as Windows Security firewall and network protection. The transcriber will be experienced with working with confidential and sensitive data, and will be subject to a confidentiality agreement. The transcriber will destroy the audio records once the transcription is done. Please see also the Appendix 10 (Data Management plan) of our Study protocol – also attached in the Data Sharing Agreement.  Appendix 10 Data Management Plan V4
15.	Who will have access to the data, and how will you ensure that access is restricted to essential users?	*Please specify teams, roles and include external organisations. In some cases, this may be named officers.* *Data must be protected to prevent unauthorised or unlawful processing.*	Each RDS is unique to a given research project and can only be accessed by users given permissions from the central IT department. The poeple who will have access to the RDS are Sarah Greene (researcher – Implementation evaluation), Jo Day (researcher – Implementation evaluation), Bekkah Bernheim (researcher-in-residence and theory lead), Lorna Stabler (principal investigator), Alankrita Singh (researcher-in-residence), Helene Prestat (project

	Question	Guidance	Response
		Please identify exactly where the information will be held on the world wide web. Distinguish between 1) servers and databases hosted entirely on council premises, 2) servers and databases in external or third-party data centres, and 3) cloud-hosted services, servers and databases. Please make sure you understand and document who will have access to the council's data. If you are not sure at this stage, mark this as a risk and be sure you find out as part of the procurement or sharing process.	manager) and Victoria Pink (transcriber – access open for only one specific folder dedicated to transcription work). Identifiable information (consent forms, verbal consent, participant attendance sheets etc.) will be kept on a secured University of Exeter SharePoint, separate from data, to ensure that data, after anonymization, cannot be linked to any individuals. Hard copies of documents such as the consent forms and attendance sheets will be scanned, stored on the secure SharePoint, and disposed of in confidential waste bins. Typed notes from interviews and audio data will be saved on a University of Exeter Research Data Storage (RDS) mapped network drive. The transcriber Victoria Pink has an ongoing relationship with researchers at the University of Exeter and is an approved supplier. Audio will be shared/uploaded to the University of Exeter RDS. The transcriber connect to RDS with a personal University of Exeter IT account following the same processes as the research team. Transcriber is accustomed to working within the boundaries of confidentiality agreements, and she has McAfee LiveSafe virus protection on her personal PC, as well as Windows Security firewall and network protection. No one else will have access to her work PC and she works alone within her home office.  Transcriber_Security Questions and answe

	Question	Guidance	Response
16.	How will you ensure that the data will be retained as per the Data / Document Retention Policy and Schedule?	*Explain how will data be retained and then deleted. Who will be responsible for deleting material – the council? Your contractor?* *Contractors and Partners:* *Ensure you have an exit strategy built it to any contractual or information sharing agreements so that you know exactly what will happen to the council's data at the end of the project/contract or information sharing arrangement*	Anonymised Findings will be summarised in report - original data used to identify cohorts will be destroyed. Anonymised findings will be shared with all participants, checked for accuracy and anonymity by the Partners In Practice Programme Lead before being published in Social Care related journals (Approved) and related recognised organisation website such as the Department of Education. Audio records held by the research team on the Exeter RDS will be deleted when the transcriptions have been returned. Anonymised Data will be retained until 31 Mar 2034. All data will be deleted from the RDS in accordance with the University Policy. The 10 years period is determined by the University Retention Policy based on stated requirements of UK Research Councils and other significant sponsors.

DPIA Change Control				
Version	Date	Nature of change	Person responsible	Role

PART THREE

Section 1. Guidance on how to complete section 2:

1. Use your knowledge of the project/procurement/ initiative, the controls that already exist, and any other contributory factors, to identify all known information (data privacy) risks.

- consider the impact of the risk on the individual whose data is processed (data subject)
- consider the risk to the council should there be an issue of non-compliance
- We have provided pre-populated guidance in the 'Privacy Risk' column as a starting point to help you identify the risks. These are based on the data protection principles under GDPR and DPA 2018 but you're not limited to the pre-populated details – you

should tailor these to the risks specific to your project/procurement/initiative and you can add more than one risk under each principle

- It is important you capture what actions you will take to reduce any identified risks to the processing of personal data. Always think of the worst case scenario and then work back on what measures could be put in place at any point in the processing (start, middle or on-going) to either prevent or reduce high risk.
- If there is nothing that can be done to mitigate high risk the council is obliged to consider consulting the Information Commissioner's Office [ICO] **before** proceeding with implementing the project. Please consult the council's DPO if this is the case.

2. Use the tables for 'Description of likelihood ratings' and 'Description of impact ratings' to objectively score the respective impact and likelihood ratings of each identified risk
3. Record your scores in the relevant column
4. Multiply the respective scores for impact and likelihood to arrive at a risk rating score for each identified risk.
5. Document the risk rating score in the appropriate column
6. Identify the controls/measures/actions you need to put in place for each risk and document them in the Mitigations column to correspond to the risk they are designed to address
7. At the end, sum up the total scores in each column and find the average of the scores for each i.e. add up all scores and divide by the number of entries for each column.
8. Once your DPIA is complete please send to the IM team or if you work in ASC/ChS/PH ensure you also send a copy to with the IG/Caldicott Support Manager to discuss. Where you have answered "no" to all the screening questions, we still advise you contact the IM team to confirm your score.
9. A record of your DPIA and score will be registered on the council's DPIA register managed by the council's Data Protection Officer [DPO] and IM Team

Understanding Risk

This section follows up on the answers you've provided in sections 1 and 2 of the DPIA.

In this section you need to assess the information (data privacy) risks that relate to the intended processing of personal data. In doing so you need to identify and assess how the possible misuse of personal data could lead to significant impacts on:

- Individuals (data subjects such as our service users, residents, staff etc.) - because their rights under data protection law are breached e.g. someone accesses their data who shouldn't. Or our poor record keeping means we are unable to find their information when they ask for it.
- The service/the council - because our processing doesn't comply with the law – e.g. we sent out a spreadsheet containing a 150 names and other information about clients to the wrong email address. This is a data breach which is potentially reportable to the ICO and could result in a fine.
-

So, we must identify the risks and what we can do to mitigate them ***before*** any personal data is used. To assist, set out below are some key risk management definitions

- A **risk** is something that may occur
- An **issue** is something that has occurred
- In calculating risk, there are two components you need to consider: *Risk = Likelihood * Impact*:
  - the **likelihood** of a risk materialising to become an issue (something that has happened = probability)
  - the **impact** that will be felt if the risk were to occur

Finally, to avoid or limit the impact, we need to think about what actions (**mitigations**) we can take to manage or plan for the future.

- A **mitigation** is a control, measure, action we can take to either stop/reduce the likelihood of the risk occurring or reduce the impact if the risk does occur (i.e. if the risk becomes an issue).

Below, there are descriptions (and their meanings) for scoring the respective Likelihood (probability) and Impact ratings – these are based on the council's Likelihood and Impact tables. Use these tables to give a rating to the likelihood and impact elements of each risk you identify

Using Likelihood and Impact Rating to Assess Data Privacy Risk

RISK FORMULA: RISK = LIKELIHOOD * IMPACT (please see section 1 Guidance on How to Complete this section)

DESCRIPTION OF IMPACT RATINGS

Impact	Descriptions
1. Very Low	•Insignificant impact to the individual or the Council •Unauthorised access to, loss or damage to ordinary personal data of up to 10 living individuals, cost impact £0 to £25,000
2. Low	•Minor impact to the individual, service or the Council •Localised decrease in perception within service area – limited local media attention, short term recovery •Unauthorised access to, loss or damage to ordinary personal data of 11-999 individuals, cost impact £25,001 to £100,000
3. Medium	•Moderate impact to the individual, service or the Council •Decrease in perception of public standing at local level – media attention highlights failure and is front page news, short to medium term recovery •Unauthorised access to, loss or damage to sensitive data of 11-999 individuals, cost impact £100,001 to £400,000
4. High	•Major impact to the individual, service or the Council, •Decrease in perception of public standing at regional level – regional media coverage, medium term recovery from incident •Unauthorised access to, loss or damage of sensitive data to over 1000 individuals, cost £400,001 to £800,000
5. Very High	•Catastrophic impact to the individual or service or the Council. For instance, Life or Death situation, shut down in service for more than 3 days – for example inability to access social care systems

DESCRIPTION OF LIKELIHOOD RATINGS

Descriptor	Likelihood Guide	Mitigations
1. **Improbable, extremely unlikely**	Virtually impossible to occur 0 to 5% chance of occurrence.	You will be required in section 4 to outline any mitigating measures that can been taken as part of the project to help justify the score given. Note: This risk may be subject to moderation following the review by the Information Management Team
2. **Remote possibility**	Very unlikely to occur 6 to 20% chance of occurrence	
3. **Occasional**	Likely to occur 21 to 50% chance of occurrence	
4. **Probable**	More likely to occur than not 51% to 80% chance of occurrence	
5. **Likely**	Almost certain to occur 81% to 100% chance of occurrence	

Section 2: Undertaking Privacy Risk Assessment: Identify all Possible Risks (Likelihood and Impact) Arising from your proposed use of the Data				
Privacy Risks	**Like-li-hood (l)**	**Impact (i)**	**Risk rating (i x l)**	**Mitigation action and other things you need to consider**
Lawfulness, Fairness, And Transparency • The data subjects (service users, customers, employees) **have not been notified (agreed/aware) to** their personal and special categories/criminal offence data being processed for the purposes of this project/procurement/initiative. If notification rather than consent, the legal basis for processing must be stated. • **We don't have a legal basis** (lawful basis for processing personal data and additional conditions for processing special categories and criminal offences data) for our proposed processing. Our proposals are not driven by statute or official requirements. It is something we would like to do, but are not obligated to undertake by law or official duty – if we are, the Public Task/Public Interest Lawful Basis should suffice ***Please note:*** *Under the GDPR* ***Consent*** *is a Lawful Basis for processing personal data in its own right. However local authorities are encouraged not to rely on it as their primary lawful basis. This is because the powers invested in local authorities are driven by statute and regulation. This means we can nearly always rely on these to justify why we undertake the processing of personal data. For example, the council cannot rely on Consent to process Council Tax Data.* *The interpretation of* ***Consent*** *within the context of performing our Public Task/Public Interest duties means that we should always endeavour to directly inform service users about how their data will be processed, what guarantees they can expect, and their rights under the GDPR - including the right to withdraw consent where there are no statutory impediments to do so*	1	3	3	No contact details will be shared and no personal data collected by the Local Authority will be made accessible without consent being obtained by the Local Authority from the participants. This will be informed by an information leaflet setting out the nature of being involved, what information will be shared and what will happen to the information shared. All conversation (interviews) will have an attached consent form that sets out they consent to the anonymised feedback being used. A process will be in place to review an individuals' consent options should they change their mind at any point. However, for the purposes of the UK GDPR, this DPIA does not rely upon explicit consent as its condition for processing. The Councils rely on Article 6.1. (e) Public Task to evaluate families experience of conferences. Article 9 (2) (j) – Archiving and Research, processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The ICPC/Alternative Pathways Evaluation gathers personal data, pseudonymises it and then anonymises the data after analysis for research purposes to help in understanding families' and professionals' journeys with the Safeguarding Family Conference. The anonymised data outputs will be

				valuable for improving families' experience with child protection work and determining the effectiveness the Family Group Conference process.
Purpose Limitation • The personal and special categories/criminal offence data sets to be handled **aren't collected for specified**, **explicit**, and **legitimate purposes**. • The personal and special categories/criminal offence data sets to be handled will **be processed in a manner that is incompatible with those purposes**. • Any future uses of the data will not be in line with the original specified purposes, and/or data subjects will not be informed of the new purposes.	**1**	**1**	**1**	No one will be asked about their personal circumstances and sharing special category information is discouraged. In the case where participants are sharing special category information, the audio records are held on a secure encrypted research data storage hub provided by the University of Exeter (RDS). No one except the research team and external transcriber will access the RDS and the researchers and transcriber will have signed a non-disclosure agreement. Once the transcription is returned, the audio record will be deleted. All data is pseudonymised and then anonymised after being analysed.
Data Minimisation • The personal and special categories/criminal offence data to be handled are **not adequate, relevant and limited** for the purposes of task in hand.	**1**	**1**	**1**	All data collected is relevant and adequate
Accuracy • The personal and special categories/criminal offence data to be handled contains **inaccuracies** that will skew the accuracy of decisions taken.	**1**	**1**	**1**	All data will be regularly checked for quality issues and any discrepancies amended and updated
Storage Limitation • The personal and special categories/criminal offence data handled is **retained** for longer than is necessary for the purposes for which it is processed.	**1**	**1**	**1**	All data will be anonymised prior to retention
Integrity and Confidentiality (Security) • Personal and special categories/criminal offence data is processed in a manner that is not secure - there is not an appropriate level of technical and organisation measures taken to protect the data against **unauthorised** or **unlawful** processing and against **accidental loss**, **destruction** or **damage**. • Assessments of suppliers and/or partners' security arrangements have not been undertaken.	**1**	**1**	**1**	Information Security have reviewed the completed 3rd Party ISQ from Exeter University and it has been approved.  20211231 3rd Party Information Assuranc

• Appropriate Information Sharing Agreements or compliance monitoring checklists have not been put in place or agreed to enable continuous monitoring of compliance controls				
Accountability • We are unable to demonstrate compliance with the data protection principles for the processing of the Personal and special categories/criminal offence data: a. Lawful, fair and transparent b. Purpose limitation c. Data minimisation d. Accuracy e. Storage limitation f. Security	**1**	**1**	**1**	All data protection principles have been considered as part of this DPIA and are compliant with the processing of this personal data.
International Transfers • Personal and special categories/criminal offence data is processed outside of the UK without appropriate safeguards in place.	**N/A**	**N/A**	**N/A**	No data will be transferred outside of the UK
Data Subject Rights • The processing of personal and special categories/criminal offence data is processed in a manner that does not comply with the rights of data subjects: 1. the right to be **informed** 2. the right of **access** 3. the right to **rectification** 4. the right to **erasure** 5. the right to **restrict processing** 6. the right to **data portability** 7. the right to **object** 8. Rights in relation to **automated decision-making and profiling**	**1**	**1**	**1**	All data subject rights will be considered under Council policy and the Council will refer to their data subject access policy for requests for information. All requests to rectify or erase will be dealt with by the Council DPO
Overall Risk Exposure Score			**10 divided**	

			by 8 = 1.25	

Section 3 – Risk Assessment and Information Management/Information Security Review
You should enter your Overall Risk Exposure Score against the appropriate Initial Score and Risk Level Box. Remember this is achieved by multiplying the impact and likelihood rates to arrive at a risk rating score for each identified risk. Add these up and then populate the initial score box. Send the DPIA to IM team for discussion and final approval.

Initial Score and Risk level			**Score**	
Low –	1- 10	Project can proceed	Yes	
Medium	11 – 15	Recommended Minor Actions Required. IM and Project to Agree Timescales		
High	16+	Recommend Significant Actions required before proceeding		

IM/IS Comments provided by: Alexandra York, 20th October 2023

To the extent of the scope of this project/ set of activities identified, a proper evaluation of Privacy and Information security risks have been done. The risks have been assessed as low. Should the scope of these activities change so that personal data will fall within scope, this DPIA must be revised to reflect that processing, reviewed by the IMT and appropriate mitigations be should adopted before IAO sign off.

IM/IS Recommended Actions

	IM/IS Recommended Action	Date Implemented
1	**No action required**	**20/4/22**
2		
3		

Final Agreed Project Risk Rating (Tick relevant box)	
Risk level	**Agreed Outcome: Closed. Open and under Review**
Low 1-10 - Project can proceed	**YES**
Medium 11-15 – Recommend minor actions are required before proceeding	
High 16+ - Recommend significant actions required before proceeding	
Please Note: All Recommended Actions will be documented on the Review section of the online DPIA register and monitored against agreed timescales. If some/all of the recommendations are not accepted this must also be captured in the Review section	

Sign off Level – Recommendation

Guidance Note on DPIA Sign Off
DPIAs should be signed off by the Information Asset Owner (IAO) for the information that will be processed.

The IAO needs to be satisfied with the level of information risk that the service area is taking
.
The IAO should be at Director or Head of Service level (the IAO role should only be devolved below that level with Director/Head of Service agreement and we would advise that this delegation is documented as part of the department's processes)

If there is more than one IAO (i.e. information will be used from more than one service area) then if all the information sits within one department the senior officer that has responsibility for the entire department may sign the DPIA off.

Where the information that will be processed comes from across the organisation then the SIRO (Senior Information Risk Owner) should sign the DPIA. However, they should only do so once the relevant Information Asset Owners have reviewed the DPIA and confirmed that they are happy for the SIRO to sign the DPIA off (the departments are still responsible for risks to their information).

If any recommendations and/or mitigations are not accepted, then this must be documented, and the signatory must capture this

This DPIA must be signed off by either IAO or SIRO whichever is appropriate (as outlined above):

Tick Box	Level
	Information Asset Owner
	Senior Information Risk Owner

Section 4. Signatories

Guidance Note – 4

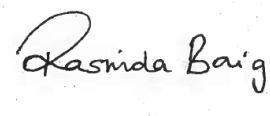
If any of the captured mitigations and IM recommended actions will not be implemented, then the signatory must capture this here and by signing they confirm they accept the additional risk posed by this.

I am satisfied that this DPIA is an accurate summary of the intended processing of personal data, the related risks and the mitigations that will be adopted.

Signature of information Asset owner

……..
Hammersmith and Fulham

Signature of information Asset owner



Rashida Baig Director of Children's Prevention, Family Help and Safeguarding Supporting People

……..
Camden