DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

Project Name	**Homes for Ukraine**	
Project Lead and Information Asset Owner/s	Project Lead	Kate Robertson (Director of Customer Service)
	IAO name and asset	Teams – Oliver Birrell
	IAO name and asset	Kate Robertson (Director of Customer Service)
Summary of the project	Due to the Ukraine crisis the government are running the homes for Ukraine programme where residents volunteer to provide accommodation for a refugee. To do this safely and securely, Camden Council is carrying out urgent checks for sponsors who have been matched with a guest in the following areas: 1. Accommodation 2. Welfare and safeguarding 3. Disclosure and Barring Service (DBS) checks As a location authority Camden Council is also administering: 4. Interim payments of £200 per refugee guest on behalf of Department for Levelling Up, Housing and Communities (DLUHC) 5. Monthly payments of £350 to sponsors as a thank you payment on behalf of DLUHC As part of this process personal and confidential information will be stored, retrieved and reported to the DLUHC (central government) who will make payments to Camden Council where a sponsor is assessed as having passed all required checks. Below are the services and leads responsible for each of these areas: a. Private sector housing service (accommodation) – [redacted] b. Early Help (Welfare) – [redacted] c. Childrens Safeguarding – [redacted] d. Floating Support (Welfare) – [redacted] e. Adult Safeguarding – [redacted] f. Human Resources (DBS) – [redacted] g. Business Support (Prepayment card) – [redacted] h. Finance (monthly sponsor payment) – [redacted]	

Implementation Date:	ASAP

Pre-screen: If you have not already done a pre-screen please do the questions below. If you have a pre-screen, attach it to the DPIA. Screening questions are to do an initial risk assessment and highlight problems that need to be addressed. Answering "Yes" to any of the screening questions above represents a potential privacy/data protection/security risk factor and the rest of the DPIA should be completed.

Q 1	Screening question	Yes/No
1.1	Does the project introduce new or additional information technologies that have privacy implications? (like facial recognition, AI?)	No
1.2	Will there be large scale systematic monitoring in a publicly accessible place – like a new CCTV system	No
1.3	Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?	Yes
1.4	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Mosaic ref, Northgate ref, and/or will use intrusive identification or identity management processes and/or electronic linkage of personal data?	Yes
1.5	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.6	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
1.7	Does the project involve new processing or significantly change the way in which personal data/special categories of personal data is handled?	Yes
1.8	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	Yes
1.9	Will data be combined, compared or matched from multiple sources?	Yes

1.10	Will you process biometric (finger print /facial recognition) or genetic data?	No
1.11	Will the personal data be processed out of the U.K?	Possibly (Ukraine Government)
1.12	Will children's personal data be processed for profiling or automated decision-making or for marketing purposes, or offering online services directly to them?	No
1.13	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.14	Will personal data be processed in a way which involves tracking individuals' online or offline location or behaviour?	No
1.15	Will personal data be processed which could result in a risk of physical harm in the event of a security breach?	Yes
1.16	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	Yes? UK Gov/potentially Ukrainian Gov in future

Step 2: What personal data is being used?										
2.1	**Is this use of personal data/special categories of personal data a new use? Or is it already happening and this is a change?**						New			
							Yes			
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Name	**X**	Date of Birth	**X**	Gender	**X**	National Insurance Number		Financial Information about the person	**X**
	Address	X	Email address	X	Telephone number	X	NHS No		Other eg a reference	X

									number such as Mosaic ref	
	Other data *(Please state):*		*Age, Languages spoken*							
	Special Categories of Personal Data									
	Racial or ethnic origin	X	Fingerprints/ Biometrics		Religious or philosophical beliefs, Political opinion					*X*
	Trade Union membership		Physical or mental health or condition							X
	Sexual life or sexual orientation	X	Housing records Social services records	X	Tax, benefit or pension records	X				
	Other data *(Please state):*		• Passport images uploaded and emailed to Camden • Passport Numbers for DBS checks. This data is also available on DLUHC (central gov) database shared with Camden • HR use an app to check that passports and other documentation are genuine as part of DBS check business as usual process (which already has a DPIA) Camden is not processing passport biometrics – this data check has already been carried out by the Home Office							
2.3	Proceedings for any offence committed or alleged, or criminal offence record?		This is not the purpose of data processing. Data provided may be required in future to support proceedings in accordance with legislation or requirements, but is unknown at present.							

Step 3: Describe the sharing/processing		
3.1	**Describe in as much detail what is being done with the data**	**a. Private sector housing service, Supporting Communities , [redacted]** **Accommodation assessment** **System used to store data: Civica APP** Data is required to enable a physical visit to the property where it will be checked for appropriateness. For example, a family with one boy aged 12 and a girl aged 10 may require three bedrooms. Disability information is required so that accessibility is assessed. **The data needed is:** Case Reference number Sponsor name Sponsor address Sponsor contact details (email and tel number) Guest/s name Guest/s date of birth and age Guest/s gender Guest/s disability information Tenure of the sponsor's home (owner/private renter/council/housing association etc). Type of property (house, flat, shed etc) **b. Early Help, Supporting People, [redacted] Welfare Check Visits – Families with children** Data is required to enable a physical visit to the property and meeting with both sponsor and guest. To record details of family members, communications needs, health needs, financial needs, adult employment and training needs, education placement needs for early years, primary and secondary school **The data needed is:** Sponsor name Sponsor date of birth and age Sponsor gender Sponsor address Sponsor contact details (email and number) Guest/s name Guest/s contact details (email and number) Guest/s date of birth and age Guest/s gender Guest address Guest/s passport

		Guest/s disability and special educational needs (SEND) information Guest/s care/support needs information **c. Childrens Safeguarding –** [redacted] Following family welfare checks carried out by the Early Help Team – in the event of child safeguarding concerns the Early Help Officer will refer to Childrens Safeguarding and a qualified social worker will investigate. All safeguarding data will be stored on the MOSAIC database and accessed by specialist service staff only with restricted access. **Data required will be as per the business as usual process via MASH and an email to the child safeguarding Ukraine lead.** **Data required: these data fields will apply to both the sponsor and household members or regular visitors to the sponsor where applicable.** Sponsor name and household member(s) if applicable Sponsor date of birth and age Sponsor gender Sponsor address Sponsor contact details (email and number) Guest/s name Guest/s contact details (email and number) Guest/s date of birth and age Guest/s gender Guest address Guest/s passport Guest/s disability information Guest/s care/support needs information Safety concerns, welfare including other needs as part of reasons for safeguarding referral **d. Floating Support –** [redacted] **Welfare check – Single Adults** Data is required to enable a physical visit to the property and meeting with both

		sponsor and guest. To record details of household members, communications needs, health needs, financial needs, adult employment and training needs The data needed is: Sponsor name Sponsor date of birth and age Sponsor gender Sponsor address Sponsor contact details (email and number) Guest/s name Guest/s contact details (email and number) Guest/s date of birth and age Guest/s gender Guest address Guest/s passport Guest/s disability information Guest/s care/support needs information **e. Adult Safeguarding –** [redacted] Following adult welfare checks carried out by the Floating Support Team – in the event of adult safeguarding concerns the Floating Support Officer will refer to Adult Safeguarding and a qualified social worker will investigate. All safeguarding data will be stored on the MOSAIC database and accessed by specialist service staff only with restricted access. **Data required will be as per the business as usual process via MASH and an email to the adult safeguarding Ukraine lead.** **Data required – these data fields will apply to both the sponsor and household members or regular visitors to the sponsor where applicable** Sponsor name and household member where applicable Sponsor date of birth and age Sponsor gender Sponsor address Sponsor contact details (email and number) Guest/s name Guest/s contact details (email and number)

		Guest/s date of birth and age Guest/s gender Guest address Guest/s passport Guest/s disability information Guest/s care/support needs information Safety concerns, welfare including other needs as part of reasons for safeguarding referral **f. Human Resources, Corporate Services, [redacted]** **DBS checks** **Will share data with First Active on their system** Documentation is collected and processed by an external company – First Active Data required: Sponsor name Sponsor gender Sponsor address Sponsor contact details (email and number) Sponsor passport Sponsor date of birth Sponsor utility bill Sponsor birth certificate Same data for sponsor's household members if applicable **g. Business Support, Corporate Services, [redacted] – Interim Payments** **Prepayment card** The following data is required to check guest identity: Sponsor name Case Reference number Sponsor date of birth Sponsor gender Sponsor address Sponsor passport Guest/s gender Guest address Guest/s passport **h. Treasury and financial services, Corporate Services, [redacted]**

		Monthly payment to sponsor for accommodation **System used: Oracle** **Data will be shared between Contact Camden Team ([redacted]) with HR** **All staff are DBS checked** Data is required to set sponsor up as supplier to receive the monthly payments. Forms will be completed monthly for payment to be made. **Data required:** Sponsor name Case Reference number Sponsor address Sponsor contact details (email and number) Bank name, account number and sort code i. **The Ukraine Contact Camden Telephone Support and Data Team ([redacted]) provide data to relevant teams across the Council so they can carry out accommodation, welfare and safeguarding visits and payments to teams above. This team also makes referrals using data on a need to know basis to other council services to meet guest needs e.g. education placement needs to Admissions Team.** The Home Office (Central government) share their Foundry database data which stores personal and sensitive data information specific to Camden based sponsors and guest refugees including passport numbers and visa data etc. The Ukraine Contact Camden Telephone Support and Data Team has direct access to this data and provides information to the teams listed above on a need to know basis so they can carry out their specific work areas.

3.2	**Explain in as much detail as possible why this is being done**		Due to the Russian invasion of Ukraine, residents are fleeing the war to other countries including the UK to safety. The UK government has set up a 'Homes for Ukraine' Scheme for residents to sponsor a refugee in their property. Homes for Ukraine: guidance for councils - GOV.UK (www.gov.uk) Camden Council is responsible for areas listed in the summary of the project above. In addition to the 'Homes for Ukraine' Scheme there is a second 'Family Visa Scheme'. Accommodation, welfare and safeguarding checks and payments are not required under this Scheme. However, support is planned to be provided by Camden Council to Camden based/destined families where systems break down, using the same or similar data sets so that the local authority can provide humanitarian support.
3.3	**Are you sharing the data with an external organisation or partner or are they involved in processing the data?**		Yes – legal duty to share outcome data with central government – Home Office and DLUHC. There is a possibly some of the data will need to be shared with other third parties such as voluntary sector organisations who can provide refugees with support, but permission will be sought from the guest in advance
	External organisation or partner Name	**Controller or Processor?**	**Is there an existing contract or Data Sharing Agreement between the council and the parties which covers information security and data protection ? No – emergency response required**
	Don't know		
3.4.	**Has a data flow mapping exercise been undertaken?**		No – this is relating to the Ukraine crisis, and is a Government run scheme. Journey map is attached

		If yes, please provide a copy, if no, please undertake
3.5	**How will the information be processed/shared**	Any data being transferred or shared with govt or 3rd party will be done so using email (Egress) or the Home Office database system called 'Foundry'

Step 4: Assess lawful basis, necessity, and proportionality			
4.1	**Identify Lawful Basis for processing personal data/special category /criminal data. Ask IRT for advice if needed (DPA@camden.gov.uk if you have no named Information Rights Officer advising)** **If not processing the category say N/A**		
	Personal data Article 6(1) UK GDPR condition Article 6(1)(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations). Article 6(1)(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law **Care Act, 2014** – legal duty to provide care and support for adults to improve their independence and wellbeing. **Children's Act, 1989** Duties to ensure children are safeguarded and their welfare is promoted.	**Special Category data UK GDPR Art 9 condition and DPA18 schedule condition** Article 9(2)(g) **processing is necessary for reasons of substantial public interest**, on the basis of 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;	**Criminal data UK GDPR Art 10 condition and corresponding art 6 condition** Data Protection Act 2018, **Schedule 1 Part 2 paragraph 18(a)(1)** (safeguarding of children and adults at risk) and **paragraph 19(2)(b)** (safeguarding of economic wellbeing of vulnerable individuals).

	Equalities Act, 2010 Duty to protect people from discrimination in the workplace and in wider society. **Rehabilitation of Offenders Act, 1974** (enhanced DBS checks)		
4.2	**If consent is a legal basis how is it obtained? Note that in most cases consent is not the basis relied on by the council. Only use consent when Information Tights Team have advised this is appropriate**		
4.3	**How will you ensure data quality and data minimisation?** If this is covered in a pre-screen refer to the pre-screen, otherwise detail below		
	See project summary and attached 'Homes for Ukraine' – data access spreadsheet.		
4.4	**Have individuals been informed about the proposed use of their data?** For example, do all the organisations/partners who will process the data inc the council cover this use in their Processing Notice online		Yes A privacy notice will be provided
4.5	**Will you comply with the council's policies on to Subject Access Requests and other data subject rights? Do contracts with any processors for the council contain the council's clauses on data subject rights?**		
	Yes		
4.6	**Will the processing of data include automated individual decision-making, including profiling?** If yes, please outline the profiling processes and the rights of the data subject		
	No – data subjects rights will be adhered to		
4.7	**Data Retention Period h***ow long will the data be kept?*		
	7 years or in accordance with regulatory/legislative framework for safeguarding data retention requirements		

Step 5: Information Security Process		
5.1	**On what systems will the data will be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	Teams private channels will be set up with restricted access for specific work area data. Private Teams Overview Spreadsheet channel with minimal required data fields so all teams can carry out visits and assessments and see if accommodation and welfare, safeguarding and DBS checks were pass/fail/in progress. Payments made to sponsor and interim payments made to refugees with dates. Each team will store detailed data e.g. family welfare checks on their own business as usual Camden Council IT systems. Early Help and Social Services will use MOSAIC. Floating Support will use HNG, Private Sector Housing Team will use CIVICA.	
5.2	**Where is the data stored geographically?**	
	UK	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
	Project summary	
5.4	Is there role based access control on all applicable systems? **How will access to information be controlled?** Teams private channels will be set up with restricted access for specific work area data.	
	Process team will have access for what	
5.5	**Is there an ability to audit access to the information?**	
	Yes – Teams channels and private channels list membership for administrators. (There is more than 1 administrator to each channel in case of leave). A spreadsheet will also be updated by the Contact Camden Telephone and Data Support Team with names, roles and access to different channels.	
5.6	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories data and/or criminal data?**	
	All officers involved in the visits and assessment process will have access to the case overview spreadsheet with minimal data and stored in a private teams channel with restricted access - as referred to in 5.1. A list of officer names with access is automatically updated in Teams in case of audit. Private teams channels will be set up for each specific work area where data needs to be stored outside of business as usual service systems. Private channels will be set up with restricted access for designated officers working within the teams as detailed in 3.1	

5.7	**Has the Information Security Manager advised on the security measures? What were his/her comments?** OK from an INFO SEC perspective. They will be using a private Teams channel.

Step 6: Identify and Assess Risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **These are the risk *before* any controls (mitigations are applied)** Add in additional rows as necessary. The completed row is an examples	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
***Misuse of data**; Personal data could be used in a manner incompatible with the Data Sharing Agreement.* *Compliance risk; Appropriate technical and organisational measures shall be taken.* *Corporate risk; Reputational risk. Loss of trust. Legal implications.*			
1. Unauthorised sharing of sponsor and refugee personal and confidential data e.g. passports, passport numbers, visa data, bank account details – for financial or personal gain e.g. financial or identity fraud.	Possible	Major	12
2. Access to private channels may be provided on request to officers who have no need to do specific related work meaning they have unnecessary access to personal and confidential data.	Possible	Minor	6

3. Sponsors sending passport images and sensitive identity data via their personal email addresses to Camden Council with no security protection vulnerable to hacking and identity fraud.	Possible	Major	12

Step 7: Identify Measures to reduce risk

Identify measures to reduce or eliminate risks identified in step 6. Remember that risks need to be reduced to an acceptable level, not all risk can be eliminated. Then calculate the risk that remains after the mitigations/controls are in place- the residual risk. Decide if this is accepted in the measure approved? column

Risk identified in step 6	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
1	Contact Camden Telephone and Data Support Team to restrict private channel and data access on a need to know basis so that officers can only access information needed to carry out their team's specific work relevant to visits, assessments and payments. Names of individual officers and access to private channels is automatically updated and available on teams in the event of audit requirement.	Unlikely	Moderate 4-6	yes
2	Private channel administrators to ensure that access is only provided to channels where officers have a specific work need. Contact Camden Telephone and Data Support Team to maintain and update a spreadsheet showing names of officers, role, work area specified, and date of access, date access deleted for audit trail.	Unlikely	Moderate 4-6	yes
3	Generic Ukraine Sponsor and Refugee inbox created as repository for personal and confidential data to be emailed to Camden Council by sponsors/refugees and then uploaded into folders on private teams channels or onto business as usual IT secure databases. Once data has been uploaded onto systems by Contact Camden the emails will be deleted twice (again in recycling) to mitigate against the risk of personal and confidential data being retrieved and used for fraudulent purposes at a later date.	Possible	Moderate 4-6	yes

Residual (remaining) risk level when all mitigations have been applied:

Medium

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	Veron Reece-Jones
DPO advice	Approved 13/4/2022 Andrew Maughan DPO and Borough Solicitor
Information Asset Owner acceptance of residual risks accepted by	Kate Robertson (Director of Customer Service)
This DPIA will kept under review by:	Kate Robertson (Director of Customer Service) Sarah Sedley (Test, Trace & Isolate – Service Manager)

Version Control

Version	Reason	Date	Author(s)
1.0			

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely
Possible	Might happen or reoccur on a semi-regular basis (no more than once a quarter)
Likely	Will reoccur on a regular basis, pointing to some failure in controls
Almost Certain	Wilful act, systemic failure in controls

Table 2 Impact of Risk if it occurs

Negligible	No personal data involved, or risk won't have any impact.
Minor	• Short-term, minimal embarrassment to an individual • Would involve small amounts of sensitive personal data about an individual • Minimal disruption or inconvenience in service delivery to an individual (e.g. an individual has to re-submit an address or re-register for a service)
Moderate	*More than a minimal amount of sensitive personal data is involved at this level* • Short-term distress or significant embarrassment to an individual or group of individuals (e.g. a family) • The potential of a financial loss for individuals concerned • Minimal disruption to a group of individuals or significant disruption in service delivery or distress to an individual (e.g. availability to a set of personal information is lost, requiring resubmission of identity evidence before services
Major	Significant amount of HR, or resident personal, and / or sensitive data released outside the organisation leading to significant actual or potential detriment (including emotional distress as well as both physical and financial damage) and / or safeguarding concerns
Catastrophic	Catastrophic amount of HR or service user personal and or sensitive data released outside the organisation leading to proven detriment and / or high-risk safeguarding concerns. Data subjects encounter significant or irreversible consequences which they may not overcome (e.g. an illegitimate access to data leading to a threat on the life of the data subjects, layoff, a financial jeopardy)

Risk Assessment: Table 3 - risk level

IMPACT	Score:	PROBABILITY				
		Rare	Unlikely	Possible	Likely	Almost Certain
	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Negligible	1	2	3	4	5

Level of risk	
1-3 Low Risk	Acceptable risk No further action or additional controls required Risk at this level should be monitored and reassessed at appropriate intervals
4-6 Moderate Risk	A risk at this level may be acceptable, if so no further action or additional controls required If not acceptable, existing controls should be monitored or adjusted
8-12 Medium / High Risk	Not normally acceptable Efforts should be made to reduce the risk, provided this is not disproportionate Determine the need for improved control measures
15-25 High Risk	Unacceptable Immediate action must be taken to manage the risk A number of control measures may be required