DATA PROTECTION IMPACT ASSESSMENT - UNITED KINGDOM RESETTLEMENT SCHEME 2020-21

Reference number:

Author: Noel Oxford
Email: noel.oxford@nottinghamcity.gov.uk

DATA PROTECTION IMPACT ASSESSMENT

When to complete this template:

Start to fill out the template at the beginning of any major project involving the use of personal data, or, where you are making a significant change to an existing process that affects personal data. Please ensure you update your project plan with the outcomes of the DPIA.

Table of Contents

1. Document Control

1. Control Details

Author of DPIA:	Noel Oxford
Owner of project:	Alex Castle-Clarke
Contact details of Author:	Noel.oxford@nottinghamcity.gov.uk

2. Document Amendment Record

Issue	Amendment Detail	Author	Date	Approved
0.1	Refresh for FY 21-22	Noel Oxford	16/03/21	

3. Contributors/Reviewers

Name	Position	Date
Mandy Pride	Senior Community Development Officer (Resettlement)	
Amy Goulden	Community Development Operations Senior Manger	
Naomi Matthews	Data Protection Officer	
Noel Oxford	Refugee Resettlement Project Officer	

Author: Noel Oxford
Email: noel.oxford@nottinghamcity.gov.uk

4. Glossary of Terms

Term	Description
UKRS	United Kingdom Resettlement Scheme
VPRS/VCRS	Vulnerable Persons' Resettlement Scheme/Vulnerable Children's Resettlement Scheme
NNRF	Nottingham & Nottinghamshire Refugee Forum
NCC	Nottingham City Council
RRF	Refugee Referral Form
PDMS	Pre-Departure Medical Screening
PEC	Pre-Embarkation Check
MHA	Migrant Health Assessment
PRA	Principal Resettlement Applicant
ESOL	English for Speakers of Other Languages
ISA	Information Sharing Agreement
RAG	Red/Amber/Green
UNHCR	United Nations High Commissioner for Refugees
DBS	Disclosure and Barring Service
NPPV2	Non-Police Personnel Vetting (Level 2)

2. Screening Questions

1. Does the project involve personal data? **Yes**	**If 'Yes', answer the questions below. If 'No', you do not need to complete a DPIA but make sure you record the decision in the project documentation.**
2. Does the processing involve any of the following data: medical data, ethnicity, criminal data, biometric data, genetic data and any other special/ sensitive data?	**Yes**
2. Does the processing involve any systematic or extensive profiling?	**No**
3. Does the project involve processing children's data or other vulnerable citizen's data?	**Yes**
4. Does the processing involve decisions about an individual's access to a product, service, opportunity or benefit that is based on any evaluation, scoring, or automated decision-making process?	**No**
5. Does the processing involve the use of innovative or new technology or the novel application of existing technologies?	**No**
6. Does this project involve processing personal data that could result in a risk of physical harm in the event of a security breach?	**Yes**
7. Does the processing combine, compare or match data from multiple sources?	**Yes**
8. Does the project involve processing personal data without providing a privacy notice?	**No**
9. Does this project process data in a way that tracks on line or off line location or behaviour?	**No**
10. Will the project involve using data in a way it has not been used before?	**No**
11. Does the project involve processing personal data on a larger scale?	**No**
12. Will the project involve processing data that might prevent the Data Subject from exercising a right or using a service or entering into a contract?	**No**
If you answered 'Yes' to any <u>two</u> of the questions above, proceed to Question 3 below. If not seek advice from the DPO as you may not need to carry out a DPIA.	**Yes**

Project Title: United Kingdom Resettlement Scheme

Team: Community Safety & Cohesion

Directorate: Community Protection

DPIA Reference number: DPIA192

Has Consultation been carried out? It is not possible to carry out resettlement according to Home Office requirements without the extensive sharing of PII. Consent for data sharing of all participants is sought at the initial application stage. NCC Data Protection colleagues have been consulted in depth, and are providing guidance and support. Any additional matters arising during the execution of this project will be recorded within this document and a new version issued.

1. DDM attached?	**No**
2. Written evidence of consultation carried out attached?	**No**
3. Project specification/ summary attached?	**Yes**
4. Any existing or previous contract / SLA / processing agreement attached?	**Yes**
5. Any relevant tendering documents attached?	**No**
6. Any other relevant documentation attached?	**Yes**

3. Project - impact on individual's privacy

Issue	Questions	Examples	Yes/No	Initial comments on issue & privacy impacts
Purpose and means		Profiling, data analytics, Marketing. Note: The GDPR requires a DPIA to be carried out where there is systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling, and on which decisions about individuals are based.		
	Please give a summary of what your project is about (*you can also attach or embed documents for example a project proposal*).			The Parties and their Representatives are working in partnership to deliver the United Kingdom Resettlement Scheme ("UKRS") which commences April 1st 2020. This is a continuation and consolidation of previous resettlement schemes, and will focus on providing an agile humanitarian response to emerging global crises, with the intent to resettle 5,000 individuals across the UK over the course of the year.
	Aims of project Explain broadly what the project aims to achieve and what types of processing it involves.			The purpose of the project is to effect local delivery of the UKRS, in accordance with a 'pledge' agreed by the Council Executive. The sharing of information is critical to this aim, as it allows us to share UNHCR documentation (including RRF and MHA, and any other best interest assessments/determinations) with NNRF, and with first-tier local authorities who are also partnered with NCC. This is so that resettled refugees can be provided with the Home Office-mandated service level of pastoral casework and support, while ensuring that all sharing of information is proportionate, secure and appropriate. NNRF are grant-funded to provide this service.
	Describe the nature of the processing How will you collect store and delete data? Will you be sharing with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are			• NCC receives all data through a secure Home Office IT portal known as Move It. • All data is stored securely in NCC servers, in the Community Safety & Cohesion shared file area. • Once cases have been reviewed and accepted, the following documentation (where applicable) will be shared with NNRF and first-tier local authorities: 1. RRF 2. MHA 3. PDMS

	involved? Who will have access to the project personal data, how is access controlled and monitored and reliability of staff assessed? Will data be separated from other data with in the system?		4. PEC • All correspondence with NNRF either utilises anonymised reference numbers, or where use of PII is unavoidable, is sent over encrypted email/Cryptshare. • All information is shared on a 'need-to-know' basis. • If any issues arise from sharing of documentation, these are resolved by phone contact between single points of contact. • All project staff are DBS and NPPV2 checked, and have completed mandatory GDPR and Information Security Awarenss training. • Data assets, including spreadsheets, registers and other tools, are securely stored and password-protected. Access is limited to essential personnel only. • Data assets are stored for as long as is strictly necessary; this timespan is expected to last until the five-year anniversary of a given individual's arrival. • Any data assets which no longer need to be retained under this policy shall be destroyed. Electronic data shall be destroyed in a manner which renders it irretrievable. Paper documents shall be immediately strip-shredded or incinerated.	
	Privacy Implications Can you think of any privacy implications in relation to this project? How will you ensure that use of personal data in the project is limited to these (or "compatible") purposes?		YES	• Data shared with NNRF are comprehensive and extremely sensitive. There are numerous implications arising from a data breach: 1. Potential for sensitive or taboo data to become known to resettled community (eg, sexuality, faith matters, various cultural taboos), potentially leading to ostracision/persecution. 2. Possibility that names/addresses of vulnerable refugees could be obtained from a data breach. Implications for Hate Crime/ASB.
	New Purpose Does your project involve a new purpose for which personal data are used?		NO	
	Consultation		YES	The Resettlement project team have consulted extensively with Data Protection colleagues extensively for practical support and

	Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals views- or justify why it's not appropriate to do so. Who else do you need to involve in NCC? Do you plan to consult Information security experts, or any other experts?			guidance. NCC has also consulted with partners around data sharing practices and implications.
Individuals (data subjects)	Will the project:	Expanding customer base; Technology which must be used by individuals; Hidden or complex uses of data; Children's data		
	Affect an increased number, or a new group, or demographic of individuals (to existing activities)?		YES	UKRS resettles refugees in groups of families, who may arrive at any given point during the year. Consequently, the number of individuals and the amount of PII stored and processed will increase as more and more refugees arrive. This increase is anticipated and managed by NCC in a manner that conforms with existing data protection practices and polices. December 2020 will mark the fifth anniversary of individuals arriving under the UKRS's prior incarnations (VPRS/VCRS), at which point PII pertaining to all such individuals will be cleansed.
	Involve a change to the way in which individuals may be contacted, or are given access to services or data? Are there any areas of public concern that you should factor in?		YES	It is possible that data processing may change the way in which an individual accesses a service; a given individual would be signposted to acute post-arrival medical attention if the MHA stated that this was needed.
	Affect particularly vulnerable individuals, including children?		YES	UKRS is designed to provide a secure route to safety for vulnerable individuals meeting specific vulnerability critera, who have been displaced by conflicts around the world.
	Give rise to a risk that individuals		YES	PRAs sign a consent declaration in their country of asylum (ie, the country from which they are resettled into the UK), which

	may not know or understand how their data are being used?			authorises UNHCR to share all information and documentation pertaining to a given family. This declaration also authorises authorities receiving this information and documentation to further share with 'appropriate settlement service agencies' (statutory or otherwise), provided a confidentiality agreement exists between all parties.
Parties	Does the project involve:	Outsources service providers; Business partners; Joint ventures		
	The disclosure of personal data to new parties?		YES	NCC works with numerous external agencies to deliver specialised aspects of UKRS. Data is disclosed on a strictly 'need-to-know' basis, therefore agencies receive only the data which is required for them to perform their task. It is possible that the exact make-up of these external agencies may change over time, according to service needs, capacities and other gaps.
	The involvement of sharing of personal data between multiple parties?		YES	NCC maintains relationships with a number of external providers, some of which will require a given level of information sharing to take place.
Data categories	Does the project involve:	Special personal data; Biometrics or genetic data; Criminal offences; Financial data; Health or social data; Data analytics: Note: the GDPR requires a DPIA to be carried out where there is processing on a large scale of special categories of data or of data relating to criminal convictions and offences		
	The collection, creation or use of new types of data?		YES	As part of case management, NCC monitors the wellbeing of families and their engagement with services. NCC maintains a 'RAG' register in partnership with NNRF, which outlines, categorises, prioritises and updates on issues resettled individuals may be facing.
	Use of any special or privacy-intrusive data involved? • Political opinions • Religious beliefs or philosophical beliefs		YES	RRF outlines details which may include: Political opinions, religious beliefs, trade union membership, genetic data, biometric daa, sexual life, prosecutions, medical data and criminal data.

	• Trade union membership • Genetic data • Biometric data • Sexual life • Prosecutions • Medical data • Criminal data (Criminal data processing, i.e. criminal convictions, etc. also has special safeguards under Article 10)			
	New identifiers, or consolidation or matching of data from multiple sources? (For example a unique reference number allocated by a new management system)		YES	Every family is allocated a unique reference number. This number is used as the primary identifier across various databases and records held by NCC.
Technology	New solutions:	Locator or surveillance technologies; Facial recognition; Note: the GDPR requires a DPIA to be carried out in particular where new technologies are involved (and if a high risk is likely)		
	Does the project involve new technology that may be privacy-intrusive?		NO	

Data quality, scale and storage	Data:	New data		
	Does the project involve changes to data quality, format, security or retention? What are the benefits of the processing? i.e. will the new system have automatic retention features? Will the system keep the information in a safer format etc.?		NO	
	Does the project involve processing data on an unusually large scale?		NO	
Monitoring, personal intrusion	Monitoring:	Surveillance; GPS tracking; Bodily testing; Searching; Note: the GDPR requires a DPIA to be carried out where the project involves systematic monitoring of a publicly accessible area on a large scale		
	Does the project involve monitoring or tracking of individuals or activities in which individuals are involved?		YES	NCC monitors families' progress as they become settled. Attendance at ESOL is considered a mandatory requirement of resettlement, so we monitor this. NCC manages a 'RAG' register of families which categorises, outlines, prioritises and updates any case management issues. NCC also seeks to monitor the outcomes of any/all intervention packages for quality and learning purposes.
	Does the project involve any intrusion of the person?		NO	
Data transfers	Transfers	Transfers outside the EEA		
	Does the project involve the transfer of data to or activities within a country that has inadequate or significantly different data protection and privacy laws?		NO	UNHCR gathers data in the second country of a resettled individual's asylum and shares this with the Home Office, which then cascades to NCC from within the UK.

4. Legal Framework and Governance – Compliance

Ref.	Question	Response	**Further action required** (and ref. to risk register as appropriate)
1. Applicable laws and regulation			
1.1	Which data protection laws, or laws which impact data protection and privacy, will be applicable to the project?	• General Data Protection Regulation 2016/679 • Data Protection Act 2018 • Human Rights Act 1998	
1.2	Are there any sector-specific or other regulatory requirements or codes of practice, which should be followed?	• Local Government Act 1972 • Localism 2011 s.1 • 1951 UN Convention Relating to the Status of Refugees • 1967 UN Protocol Relating to the Status of Refugees • Asylum and Immigration Act 1996	
2. Organisation's policies			
2.1	Is the project in compliance with the organisation`s information management policies and procedures (including data protection, information security, electronic communications)?	Yes.	

2.2	Which policy requirements will need to be followed throughout design and implementation of the project?	Data Protection Policy Information Security Policy Records Management Policy	
2.3	Are any changes/updates required to the organisation`s policies and procedures to take into account the project? **Note: new requirements for *"Accountability"* under the GDPR, including record-keeping, DPOs and policies**	Yes	• Action plan in respect of data retention. • Review whether NCC standard policy is appropriate. • PRA has signed consent; not clear what other family members understanding of their rights is.
3. Training and roles			
3.1	Will any additional training be needed for staff in relation to privacy and data protection matters arising from the project?		• NCC training and procedures compliant. • NNRF would benefit from more rigorous data practices.

5. Personal Data Processing Compliance

Ref.	Question	Response	Further action required (and ref. to risk register as appropriate)
1.	**Personal Data Processing**		
1.1	Which aspects of the project will involve the processing of personal data relating to living individuals?	• Consideration of cases. Initial referral is anonymised, but often the full document is required for a decision. • Property matching. Effort is made to consider an individual's (and family's) whole life circumstances in deciding which properties are appropriate. • After arrival, individuals are monitored for safeguarding and case management purposes, in accordance with Home Office requirements.	
1.2	Who is/are the data controller(s) in relation to such processing activities?	NCC	
1.3	Who is/are the data processor in relations to such processing activities?	NNRF	
2.	**Fair and Lawful processing - GDPR Articles 5(1)(a), 6, 9, 12, 13**		
2.1	Which fair processing conditions are you relying on? GDPR: Article 6(1) (legal basis for processing) and, for sensitive personal data, Article 9(2).	6(1). **Choose at least one of the following for personal data**, **usually (e)**-(Cross out the rest) ~~a) Consent~~ ~~b) Performance of contract~~ ~~c) Legal obligation~~ ~~d) Vital interests~~ **e) Public interest / exercise of Authority** 9(2) Choose at least 1 for special data-usually g (cross the rest out) a)Explicit consent	

		b) ~~Employment / social security / social protection obligations~~ c) Vital interests ~~d) Non-profit bodies~~ ~~e) Processing made public by data subject~~ ~~f) Legal claims~~ ~~g) Substantial public interest~~ ~~h) Health, social care, medicine~~ ~~I) Public interest for public health~~ ~~j) Archiving, statistics, historical research~~ **For any criminal Data** Comply with Article 10 **if it meets a condition in Part 1, 2 or 3 of Schedule 1.** • ~~Employment, social security and social protection~~ • ~~Health and social care purposes~~ • ~~Public health~~ • ~~Research~~ • ~~Substantial public interest:~~ • ~~Statutory and government purposes~~ • ~~Equality of opportunity and treatment~~ • ~~Racial and ethnic diversity at senior levels of organisations~~ • ~~Preventing or detecting Unlawful Acts~~ • ~~Protecting the public against dishonesty etc~~ • ~~Regulatory requirements relating to unlawful acts and dishonesty etc~~ • ~~Journalism etc in connection with unlawful acts and dishonesty etc~~ • ~~Preventing fraud~~ • ~~Suspicion of terrorist financing or money laundering~~ • ~~Counselling~~	

		• Safeguarding of children and of individuals at risk • ~~Safeguarding of economic well-being of certain individuals~~ • ~~Insurance~~ • ~~Occupational pensions~~ • ~~Political parties processing~~ • ~~Disclosure to elected representatives~~ • ~~Informing elected representatives about prisoners~~ Additional Conditions • ~~Consent~~ • Vital interests • ~~Personal data in the public domain~~ • ~~Legal claims~~ • ~~Judicial Acts~~	
Note: different conditions may be relied upon for different elements of the project and different processing activities. Also, the scope of special category data is wider under the GDPR, and in particular includes genetics & biometric data, and sexual orientation.			
2.2	How will any consents be evidenced and how will requests to withdraw consent be managed?	• PRA in each case signs a declaration of consent for the UNHCR and other resettlement agencies (statutory or non-statutory) to share personal data. • Requests to withdraw consent would amount to a request to withdraw from the scheme. In this instance, NCC would cease any and all activities around the family, and would purge all relevant data.	
Note: new requirements for obtaining and managing consents within the GDPR.			
2.3	Is the data processing under the project covered by fair processing information already provided to individuals or is a new communication needed (see also data	Attach privacy notice or provide a working link to the relevant privacy notice	It is unclear how information was conveyed pre-departure. As such there is a case for providing supporting messages

	subject rights below)?		around individual rights in respect of data.
Note: more extensive information required under the GDPR than under current law, and new requirements on how such information is provided. Also a general principle of "*transparency"*. It is important to assess necessity and Proportionality			
2.4	If data is collected from a third party, are any data protection arrangements made with such third party?	Yes	
2.5	Is there a risk of anyone being misled or deceived?	No	
2.6	Is the processing "fair" and proportionate to the need's and aims of the projects?	Yes	
2.7	Are these purposes clear in privacy notices to individuals? (see above)	Yes	

3. Adequate, relevant and not excessive, data minimisation - GDPR Article 5(1)(c)			
3.1	Is each category relevant and necessary for the project? Is there any data you could not use and still achieve the same goals?	Yes. No.	
Note: GDPR requires data to be "limited to what is necessary" for the purposes (as well as adequate and relevant).			
3.2	Is/can data be anonymised (or pseudonymised) for the project?	Each family has a unique identifying number, individuals may be referred to by initial, or by position within the family. Such instances are never linked to data such as addresses, etc	
4. Accurate and up to date - GDPR Article 5(1)(d)			
4.1	What steps will be taken to ensure accurate data is recorded and used?	NCC is reliant on third-party data collection in most instances. Where inaccuracies are noted, NCC will rectify these on existing systems and will feed back details of the inaccuracy. NCC endeavours to maintain up-to-date data records, and works closely with NNRF to maintain shared management tools,	

		such as the 'RAG' register.	
For example: checks when receiving/sending information from/to third parties, or transcribing information from oral conversations or handwritten documents, any automatic checks on information not meeting certain criteria.			
4.2	Will regular checks be made to ensure project data is up to date?	Data is regularly consulted and checked for accuracy as financial benchmarks are dependent on accurate records.	
5. Data retention - GDPR Article 5(1)(e)			
5.1	How long will personal data included within the project be retained?	Five years from date of arrival	
5.2	How will redundant data be identified and deleted in practice? Consider paper records, electronic records, equipment?	No paper records are retained. Electronic records are stored in various databases, which will be purged in line with the retention policy. Referral documentation, 'RAG' register and initial provision planning tools containing the most sensitive issues can simply be deleted or updated as applicable. Financial planning tools can be anonymised once all claims have been remitted.	Is there an argument for sharing exit data with other agencies in cases of concern?
5.3	Can redundant data be easily separated from data which still need to be retained?	Datapoints are captured in a sufficiently granular fashion as to enable this.	
6. Data subject rights - GDPR Articles 12 to 22			
6.1	Who are the relevant data subjects?	Refugees resettled in the UK under the UKRS.	
6.2	Will data within the project be within the scope of the organisation`s subject access request procedure?	Yes	
6.3	Are there any limitations on access by data subjects?	All access would be in line with relevant NCC FOI/SAR policies	
6.4	Is any data processing under the project likely to cause damage or distress to data subjects? How are notifications from individuals in relation to damage and distress managed?	No	
6.5	Does the project involve any direct marketing to individuals? How are	No	

	requests from data subjects not to receive direct marketing managed?		
6.6	Does the project involve any automated decision making? How are notifications from data subjects in relation to such decisions managed?	No	
6.7	How will other rights of data subjects be addressed? How will security breaches be managed?	These rights will be processed by the Information Compliance Team at Nottingham City Council. All breaches will be dealt with by the Information Compliance team and the Data Protection Officer.	

7. Data Security - GDPR Articles 5(1)(f), 32

For example:

- **Technology**: encryption, anti-virus, network controls, backups, DR, intrusion detection;
- **Physical**: building security, clear desks, lock-leads, locked cabinets, confidential waste;
  Organisational: protocols on use of technology, asset registers, training for staff, pseudonymisation, regular testing of security measures.

Describe the source of risk and nature of potential impact on the individuals. Include associated compliance and corporate risks as necessary -What security measures and controls will be incorporated into or applied to the project to protect personal data? Consider those that apply throughout the organisation and those which will be specific to the project. N.B Measures that are appropriate to the nature of the data and the harm which may result from a security breach	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant or Severe	**Overall Risk** Low, Medium or High
• NCC stores data in Excel, Word or pdf files on internal servers. Sensitive data is protected by password and accessible only to NPPV2 vetted colleagues. • Email containing sensitive information is encrypted. Names are initialised or replaced with a reference. • Community Protection enforces a clear desk	Remote Remote	Significant Minimal	Medium Low

policy. Computers are locked in user absence, and stored securely in lockers outside working hours. • Printed material containing sensitive data is retained only as long as required, and destroyed as confidential waste.	Remote Remote	Minimal Minimal	Low Low
Identify measures to Reduce Risk- Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk that you have identified			

Risk	Options to reduce or eliminate risk	**Effect on risk** Eliminated/ Reduced or Accepted	**Residual risk** Low/Medium/High	**Measures approved** Yes/No
Personal data stored in digital form by NCC is accessed without authorisation	Files are password protected on multiple levels. Strong passwords are used. UKRS data is no more vulnerable than anything else on NCC servers.	Reduced	Medium	
Personal data in physical form is seen by an unintended recipient	NCC avoids using printed data to the greatest extent. As soon as any such documents have served their purpose, they are destroyed as confidential waste.	Reduced	Low	
Email could be sent to the wrong recipient	NCC encrypts all sensitive emails. Sensitive files are password-protected and sent via Cryptshare, with the password supplied by separate email. Autofill options are turned off to prevent accidental inclusion of extraneous email addresses.	Reduced	Low	

8. Data processors - GDPR Article 28 & direct obligations in other articles			
8.1	Are any data processors involved in the project?	Yes	
8.2	What security guarantees do you have?	Signed ISA	
For example: specific security standards or measures, reputation and reviews			
8.3	Please attach the processing agreement		
For example: security terms, requirements to act on your instructions, regular audits or other ongoing guarantees Note: new requirements for the terms of contracts under the GDPR (much more detailed than current law).			
8.4	How will the contract and actions of the data processor be monitored and enforced?	Power to audit under the processing agreement.	
8.5	How will direct obligations of data processors be managed?	Under the processing agreement	
Note: New direct obligations for processors under the GDPR, including security, data protection officer, record-keeping, international data transfers.			
For example: fair & lawful, lawful purpose, data subject aware, security, relevance.			
9. International data transfers - GDPR Articles 44 to 50			
9.1	Does the project involve any transfers of personal data outside the European Union or European Economic	No	

	Area?		
9.2	What steps are taken to overcome the restrictions?	N/A	
For example: Safe Country, contractual measures, binding corporate rules, internal assessments of adequacy Note: GDPR has similar methods to overcome restrictions as under current law, but there are differences to the detail and less scope for an "own assessment" of adequacy.			
10. Exemptions			
10.1	Will any exemptions for specific types of processing and/or specific DP requirements be relied upon for the project?	No	
For example: crime prevention, national security, regulatory purposes Note: Exemptions under the GDPR to be assessed separately, and may be defined within additional EU or UK laws.			

6. Sign off and record outcomes

Item	**Name**	**Date**
Measures approved by: (project owner) This must be signed before the DP can sign off on the DPIA.	Amy Goulden	18/03/21
Residual risks approved by: (If accepting any residual high risk, consult the ICO before going ahead)	Amy Goulden	18/03/21
DPO advice provided: (DPO should advise on compliance, measures and whether processing can proceed)		
Summary of DPO advice:		
DPO advice accepted or overruled by		If overruled, you must explain your reasons
Comments:		
IT Security Officer: Where there are IT security issues		
IT Officer comments:		
SIRO Sign off: (For major projects)		
Consultation responses reviewed by:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA