The London Borough of Camden adopt this Data Protection Impact Assessment Form as their own, with addition of the risk assessment Appendix 3. References to CoL's policies etc should be read as LBC's.

Data Protection Impact Assessment Form

Title: Agency Staff Fraud Risks – London Fraud Hub Data Matching Project

When to complete this form

The form should be completed at the start of any project that is considering the processing of personal data and special personal data. It **must** be completed where there is a high-risk to the processing of personal data – see section 2.

Definitions

Personal data is that which can identify a living individual and is typically (but not exclusively) photographs, names, addresses, email addresses, date of birth, passport, payroll number.

Special category data (previously referred to as sensitive data) is typically racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health sex life, or biometric / genetic data. *Please refer to section 5 of this form.*

Data Controller is the public authority, individual, organisation etc. who determines the purposes and means of the processing of personal data.

Data Processor only processes personal information on behalf of a Data Controller.

Sub-Processor is a organisation /company/ third party who work on behalf of the data processor and process personal data for them.

Independent Controller are data controllers in their own right. They do not share the same personal information and nor do they act together to decide how personal information should be processed. All data controllers remain independently responsible for compliance with controller obligations under the GDPR.

Joint Controllers act together to decide the purposes and means of the processing. They often have shared purposes i.e. law enforcement.

1. Screening Questions

If you answer yes to one or more of the following questions, you should complete sections 2-8.

Is the DPIA required as part of a tender process for a contract?	Yes☐	No☒
Will the project involve use of new technology or software to process personal and/or special category data? Note*: Even though some sources may not contain personal data, when combined with other data sets used these may create a new data set that will enable an individual to be identified.*	Yes☒	No☐
Will the project match or combine data from different sources?	Yes☒	No☐
Will the project use information on the habits of individuals to suggest services and/or products to match these habits? (this is referred to as profiling)	Yes☐	No☒
Will the project involve processing of special category or criminal offence data?	Yes☐	No☒
Will the project involve the use of CCTV?	Yes☐	No☒
Will the project involve the systematic monitoring of a publicly available area on a large scale i.e automatic number plate recognition, intelligent transport systems, traffic management systems involving monitoring of vehicle/driver behaviour, Wi-Fi/Bluetooth tracking	Yes☐	No☒
Will the project involve profiling or special category data to decide on access to services?	Yes☐	No☒
Will the project process biometric data such as fingerprints or facial imaging?	Yes☐	No☒
Will the project process genetic data?	Yes☐	No☒
Will the project collect personal data from a source other than the individual(s) without providing them with a privacy notice? ('invisible processing')	Yes☐	No☒
Will the project involve tracking an individuals' location or behavior?	Yes☐	No☒

Will the project profile children or target services at them?	Yes☐	No☒
Will the project process data that might endanger the individual's physical health or safety in the event of a security breach?	Yes☐	No☒

2. Risk Management – Personal Data

Note: These risks are not the same as risks to project delivery. If you identify a high-risk you must send a copy of this form to the Data Protection Officer : Michael.Cogher@cityoflondon.gov.uk

Examples of processing that could result in a high risk include

- where consent has not been given
- the introduction of new technologies
- projects where no Data Protection Impact Assessment has been carried out before by the controller
- where a new DPIA has become necessary in the light of the time that has elapsed since the initial processing
- high risk data such as special personal data or data that involves children and safeguarding concerns

Identify any risks to the Processing of Personal / Special Category Data.	Describe the Action You Will Take to Mitigate the Risk
There is a risk that an external attacker gains access to personal data.	The contractor, Synectic's who provide the NFI and NFI fraud hub systems has ISO 27001 accreditation. The NFI environment at the supplier is accredited against government standards annually - including penetration testing and IT Health Checks undertaken by specialist 3rd party company. All relevant staff at Synectic's are security cleared. All data transmissions (unless an exception is approved) are via the secure NFI environment. A full incident response plan is in place.
There is a risk that information could be lost, released or shared inappropriately	Controls are per the above
There is a risk that data disclosed are not required for the purposes of fraud detection, or are excessive.	The data required from participants will be the data that is adequate, relevant and limited to what is necessary to undertake the matching exercise; to enable the accurate identification of Individuals; to report results of sufficient quality; and to meet the purpose of preventing and detecting fraud.

There is a risk that data is retained longer than is necessary for the purposes of NFI	The NFI has published a data deletion schedule. The Data Deletion Schedule applies to the NFI data matching exercises. Our IT contractor provides certificates of deletion. This Data Deletion Schedule covers all proof of concept (research and development) data matching unless a specific timetable has been approved and documented as part of the proof-of-concept project scoping.
There is a risk that people will be misidentified as a result of data processing	The Cabinet Office, working with Synectics and participants has built up a robust series of matching rules that aim to identify the same (or different as applicable when carrying out address matching) individual across multiple data sources. NFI participants are informed to check all matches and ensure that ID is certain before taking any action and have regard to sensitive matches such are those to deceased or vulnerable people
There is a risk that personal data will be used for purposes other than those intended	Participants' use of the NFI data is governed by the NFI Code of Data matching Practice In addition to this Code, when participating in data matching exercises, bodies should have regard to any other relevant data or information sharing codes and guidance, including any statutory guidance from the Information Commissioner. London Boroughs have clearly set-out the purpose for how the data will be used and it is clear with the NFI team at the Cabinet Office and Synectic's. The Cabinet Office has a Governance Board in place that signs off all data matching including proof of concept work. With a representation from Cabinet Office Legal Services.
There is a risk that a data subject is not informed about the use of their personal data	The Cabinet Office Code of Data Matching Practice sets out that participants must comply with data protection legislation. This requires that data must be processed lawfully, fairly, in a transparent manner and for specified and legitimate purposes. In addition, data controllers must inform individuals that their data will be processed. All London NFI Fraud Hub participants are required to complete and agree with their respective Information Teams, a DPIA and achieve sign-off. London Boroughs are required to ensure their privacy notices accurately reflect the use of personal data for the detection and prevention of fraud. Participating bodies must provide a written notice, known as a privacy notice, which contains the information required by data protection legislation. Participants must submit a declaration confirming compliance with the privacy notice requirements to the Cabinet Office.

	The Cabinet Office NFI Team monitor submission of these declarations to ensure they are completed in the required timescale. If the Cabinet Office becomes aware that privacy notice requirements have not been adhered to, it will agree the steps necessary for the participant to achieve compliance. The Cabinet Office may seek input from the Information Commissioner as part of this process. The Cabinet Office has a privacy notice for the NFI. This notice sets out how we will use personal data, and a data subjects rights. It is made under Article 14 of the General Data Protection Regulation (GDPR).
There is a possibility that a member of the NFI participants staff may seek to cause harm through disclosure of personal information	A NFI Security Policy is in place and participants must confirm their compliance. All users should have undergone appropriate pre-employment screening checks to ensure that the threat to the system or the information is mitigated as far as possible. This includes any subcontractors, third parties or temporary staff that will be using the system on behalf of the organisation. It is recommended that the following standard (or equivalent) is adhered to: HMG Baseline Personnel Security Standard.
There is a risk that a data subject's data is inaccurate	Once data is received it is quality checked by Synectic's, and, if it is found to be inaccurate, a request will be made for resubmission of that data. We will work with our recruitment agency/managed service provider partners to ensure that data is correct, where this may be found to not be the case. We inform the data subject they have the right to rectification on our privacy notice.

3. Data Protection Principles

Describe how the Project Conforms to the Six Data Protection Principles	
1. Shall be processed lawfully, fairly and in a transparent manner in relation to the data subject e.g. where there is a privacy notice in place.	The Cabinet Office (CO) are the owners of the NFI, the NFI IT system is provided to the CO under a contract by Synectics Solutions, data provided for this initiative will be processed by Synectics within the NFI system. The data matching is undertaken for the prevention and/or detection of crime. Please see appendix one for a copy of the Code of Data Matching Practice that is being used for this activity. Only data matches, suggesting a concern for further investigation regarding multiple working will be shared

	through the NFI secure site with London NFI Fraud Hub members. London NFI Fraud Hub members, of which the City Corporation is one will process personal data for the prevention and/or detection of crime. There are relevant privacy notices in place, and these will be reviewed periodically. Personal Data is shared and processed by the NFI, under the provisions set out in Part 6 of the Local Audit and Accountability Act 2014. Privacy notices are in place for all NFI data-set areas, furthermore, a privacy notice, published by the NFI team is available on the City's internet and intranet, and referred to within NFI data-set areas. The NFI Privacy Notice can be found here, whilst the City's NFI Internet page links to the NFI information on the .gov website. As the processing is undertaken under Part 6 of the Local Audit and Accountability Act 2014, the processing is lawful for NFI and NFI Fraud Hub data-matching purposes. Each local authority who have signed up to this activity will be responsible for providing their own satisfactory privacy notice.
2.Shall be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.	Part 6 of the Local Audit and Accountability Act 2014, allows the NFI data matching for the purpose of the prevention and detection of fraud – this includes matching for the purpose of the NFI Fraud Hub. Data will be processed by the NFI for these purposes and for statistical purposes for example stats being reported to Audit & Risk Committee for example.
3. Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.	The data-specifications detail the personal data fields used for data matching within the NFI Fraud Hub for data-matching purposes. Only the data specified within the data specifications will be used for NFI Fraud Hub purposes.
4. Shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.	Where inaccurate data is identified, we will take steps to erase or rectify with the appropriate owning department as appropriate. We have mechanisms in place to identify if data is inaccurate and this may be from identification through third party intelligence, such as credit reports accessed as part of a fraud investigation, or through a report from a department following engagement with a member of the public for example. The NFI

	(https://www.cityoflondon.gov.uk/about-us/access-to-information/national-fraud-initiative) Privacy notice, which is also included on the City's website, has contact details for the Internal Audit team who manage the NFI for the City and this mechanism can be used for an individual to contact us regarding rectification or erasure.
5. Shall not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed. Personal data may be stored for longer periods provided it is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This is subject to the implementation of appropriate data security measures designed to safeguard the rights and freedoms of data subjects.	The NFI data retention periods can be found online here. For the purpose of the proof-of-concept stage (October 2023 to April 2024) the retention period will be six months.
6. Shall be processed in a manner that ensures its appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.	Data shall only be processed through the NFI secure site, which has a number of safeguards in place: all data is processed within the NFI secure site, which has a number of safeguards in place to restrict access, including passwords and two factor authentication via text or email, with regular enforced changes to passwords, management of user accounts by the Key Contact and account suppression in the event of no access after 90 days.

3b) Describe the sharing/processing.

List of organisations/third parties/partners involved with sharing or processing the data for this activity.

Name	Data Controller	Data Processor	Independent controller	Joint Controller	Sub-processor
Recruitment agencies and managed	☐	☒	☒	☐	☐

service providers					
London boroughs	☒	☒	☐	☐	☐
Cabinet Office NFI team	☐	☒	☐	☐	☐
Synectics Solutions	☐	☒	☒	☐	☐
City of London	☒	☐	☐	☐	☐

Is there a Contract/ Data sharing agreement in place for the above? Please add in more rows if needed.

Name of parties to the contract/ data sharing agreement	**Contract**	**Data Sharing Agreement**	**Other (please provide details)**
City of London – Cabinet Office for Synetics	☒	☐	
City of London – those participating	☐	☒	

Describe in as much detail why this information is being processed/shared/viewed?

The fraud risk being tackled by this project is polygamous working, this is a common risk across London boroughs, and we are using the NFI London Fraud Hub to tackle this fraud by matching council payroll data and recruitment agency/managed service provider data to identify where workers/employees may be working for more than one council at any one time.

The London Borough Fraud Investigators Group (LBFIG) is overseeing the network for this initiative and has brought together NFI London Fraud Hub members, recruitment agency/managed service provider, the CO's NFI team and Synectic's to kick start this project.

Data provided by NFI London Fraud Hub members and recruitment agency/managed service providers will be processed through the NFI London Fraud Hub, thereby reducing the need for councils to hold more data than is necessary. Only data matches indicating that workers/employees may be working for more than one organisation at any one time will be shared with those appropriate councils for further investigation. For example:

Worker X at CoL matched to Worker Y at RBKC – both CoL and RBKC will see both sides of the match. Worker X at CoL matched to Worker Y at RBKC and Worker Z at LBWF – CoL, RBKC and LBWF will see both sides of the match. In order to investigate appropriately it is essential that the participants see this data.

4. Project Details.

Project Name : Agency Staff Fraud Risks – London Fraud Hub Data Matching Project

Start Date: proof-of-concept period	October 2023	End Date	April 2024
		Recurring / Ongoing ?	Yes, subject to review of POC
If recurring or ongoing, will the DPIA need updating ? Yes If so, how will this be done ? We will review the DPIA to ensure that it remains fit for purpose, post the POC period. Post POC the DPIA will be reviewed annually and when any changes occur to this activity.			
Project Manager Contact Details	Name : [redacted] Email : [redacted]		
Supporting Comments			

Project Objectives (from the PID)

Participation in the NFI Fraud Hub is an additional and chargeable tool, designed to identify fraud at an earlier stage and mitigate the risks of losses from fraud to local authorities. objectives are to ensure that the processing of data for NFI fraud hub purposes are lawful and that data subjects are provided with sufficient information regarding the NFI activity. The datasets covered by the NFI fraud hub mirror those of the biennial exercise and as such are covered within this FPN's for NFI data-matching. The NFI Fraud Hub also allows for additional data matching, outside of the standard datasets, to identify new and emerging fraud risks. This project is an extension of the Payroll to Payroll data matching, with recruitment agencies/managed service providers sharing data with the NFI London Fraud Hub on a voluntary basis.

Vendor Name, Address and Contact Details :

The NFI team are part of the Cabinet Office, Cabinet Office, 70 Whitehall, London, SW1A 2AS, the key contact details for the NFI Team are:
Email address: nfiqueries@cabinetoffice.gov.uk
Telephone: 0845 345 8019

Contract Term: Cabinet Office – system

Start Date:		End Date:	
		Optional extension period (years):	

Contract Term: Data Sharing Agreement

Start Date:		End Date:	
		Optional extension period (years):	

5. The Data / Data Subjects (the person(s) to whom the data relates)

Describe the data/ list the fields

What items of data are being processed and what type of data are they i.e special category or personal

Data	Format	Type of Data
Payroll data		
Payroll data - name	Excel	Personal
Payroll data - address	Excel	Personal
Payroll data - email addresses	Excel	Personal
Payroll data – dob	Excel	Personal
Payroll data - bank account	Excel	Financial
Payroll data – NiNo	Excel	Personal
Payroll data - telephone number	Excel	Personal
Payroll data - reference numbers	Excel	Personal

(add additional entries as required)

Comments:

Details of all data specifications and data fields required, can be found in the NFI data specifications - https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-specifications

'Special Categories' of Personal Data

Tick a box if the Personal Data processed fits into a relevant 'Special Category' below.

Religion or beliefs	☐	Genetic data	☐
Race or ethnic origin	☐	Health	☐
Political opinions	☐	Sexual orientation	☐
Trade-union membership	☐	Criminal convictions	☐

Categories of Data Subject

Tick a box next to the categories of data subject whose personal data will be processed

Customers	☐	Complainants (& Reps)	☐	Suspected Offenders	☐
Suppliers	☒	Advisors/ Consultants	☒	License/ Permit Holders	☐
Offenders	☐	Benefits Recipients	☐	Tenants / Residents	☐
Claimants	☐	Carers (& Reps)	☐	Captured on CCTV	☐
Students/ Pupils	☐	Incident witnesses	☐	Employees of other Orgs	☒
Landlords	☐	Employees/ Contractors	☒	Holders of Public Office	☐

Supporting Comments: Data subjects for this project are:

- Council Employees (permanent, casual, FTC etc)
- Recruitment Agency workers
- Managed Service Provider workers

6. Conditions for data processing

(Tick all relevant conditions which provide the legal basis for the processing of personal and /or special category data)

Conditions for Processing

Personal Data			Special Categories		
6(1)(a)	Consent	☐	9(2)(a)	Explicit Consent	☐
6(1)(b)	Contracts	☐	9(2)(b)	Employment, Social Security, Social Protection law	☐
6(1)(c)	Legal obligation	☒	9(2)(c)	Vital interests	☐
6(1)(d)	Vital interests	☐	9(2)(d)	Not-for-profit body	☐
6(1)(e)	Public Interest/ Official Authority	☒	9(2)(e)	Made public	☐
6(1)(f)	(not applicable to Public bodies)		9(2)(f)	Legal claims / Judicial	☐
			9(2)(g)	Public Interest	☐
			9(2)(h)	Medicine, Employee capacity, Medical Diagnosis, Health or Social Care	☐

	9(2)(i)	Public Health	☐
	9(2)(j)	Archiving, Scientific and Historical Research or Statistical Purposes	☐

Consent for Processing

If consent / explicit consent is being relied upon, attach evidence of consent to this document	☐
Comments:	
• **Not applicable**	

Training in how to securely process the data

Confirm that employees (and users where relevant) of the system have received appropriate data protection training	☒
Confirm that comprehensive written guidance will be available to employees and users	☒
Comments:	
• Historic NFI users are familiar with the NFI system and data security requirements. Any new NFI users will be required to undertake training via the NFI secure site. • All CoL staff with access to this system have completed the mandatory Data Protection E-Learning,	

Data Security Access controls

Confirm who has read only access to the data and the business reason for this
Confirm who has permissions to view, create, amend and delete data and the business reason for this
Comments:
• The Counter Fraud & Investigation Manager is the NFI Key Contact and manages NFI secure site access, along with the permissions for CoL users, these are defined as appropriate for each NFI user with restricted access to matches as needed for official business.

Securing the data within a system	
Confirm that appropriate technical security (i.e. restricted logins) is in place to protect the data at risk from threats	☒
Comments:	
• Only users assigned with an account can access the NFI secure site, the NFI secure site has inbuilt security to mitigate the risks of unauthorised access and an audit log of any unauthorised attempts is monitored by the Key Contact.	

Securing the data when transferred from one system to another	
Confirm that appropriate technical security is in place to protect the data in transit from threats	☒
Comments:	
• Only users assigned with an account can access the NFI secure site, the NFI secure site has inbuilt security to mitigate the risks of unauthorised access and an audit log of any unauthorised attempts is monitored by the Key Contact.	

7. Data Subjects Rights

A very brief description of each right is included in the table below. More detail can be found in the CoL Data Subjects' Rights Policy.
https://corpoflondon.sharepoint.com/sites/Intranet/_layouts/15/search.aspx/siteall?q=Data%20Subject%20Rights%20Policy

Please tick appropriate box against each section to confirm which individual rights apply in the processing of personal data.

If you have any further queries, please contact information.officer@cityoflondon.gov.uk

Right to be informed CoL as a data controller must ensure that when collecting personal data, detailed information in the form of a privacy notice is made available to data subjects,explaining why and how personal data is being collected / used.	Yes☒	No☐	N/A ☐
Right to access (also known as 'subject access requests') This right of access permits data subjects to obtain confirmation from the data controller as to whether or not it is processing their personal data, and where that is the case, obtain access to their personal data.	Yes☒	No☐	N/A ☐
Right to rectification Data subjects have the right to correct inaccurate personal data about them processed by a data controller and/or update	Yes☒	No☐	N/A ☐

personal data about them processed by a data controller, where that personal data is incomplete.			
Right to erasure ("Right to be forgotten") Data subjects have the right, in certain circumstances, to request the erasure of their personal data.	Yes☒	No☐	N/A ☐
Right to restriction Data subjects have the right, in certain circumstances, to restrict the processing of their personal data by a data controller.	Yes☒	No☐	N/A ☐
Right to data portability Data subjects have the right to be provided with their personal data in a structured, commonly used and machine-readable format, which they can store for further personal use. This right also permits data subjects to request that a data controller transmits this personal data to another data controller of the data subject's choice	Yes☒	No☐	N/A ☐
Right to object Data subjects have the right to object to the processing of their personal data by a data controller, requiring them to cease the processing in certain circumstances	Yes☒	No☐	N/A ☐
Right to object to automated decision-making and profiling Data subjects have the right to object to their personal data being used in automated decision-making processes or for profiling: • Automated Decision Making: making a decision solely by automated means without any human involvement • Profiling: automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.	Yes☒	No☐	N/A ☐

8. Transfer of Personal Data Outside of the UK

Transfer of Personal Data Outside of the UK	
No personal data will be transferred to third countries.	☒
It will be necessary to transfer personal data to third countries and the Data Protection Officer has been notified.	☐
The data will be securely transferred using one for more of the following safeguards https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/	

Comments:
• Data is only held in UK data storage centres

If you assess there is a risk in transferring this data, you should notify the Data Protection Officer.

9. Approval

SEE LBC APPENDIX 3

10. Distribution

A copy of the completed form must be logged and retained by the data owner.

Further copy should be sent to the Compliance Team information.officer@cityoflondon.gov.uk who will log and retain this form as a central record, which will be available on request for scrutiny by relevant person(s)

11. Version Control

Version Control	Date	Notes/Changes
V0.1	12/09/2023	IA Comments
V0.2	12/09/2023	Compliance Team comments
V0.3	13/09/2023	Compliance Team and IA Comments following meeting.

12 – appendices

Appendix 1 – Code of Data Matching Practice

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/750372/Code_of_Data_Matching_Practice.pdf

Appendix 2 - DPIA for NFI (LBC note this will be published on our Data Portal DPIA (Data Privacy Impact Assessments) | Open Data Portal (camden.gov.uk))

Appendix 3- LBC Risk Assessment

APPENDIX 3

• DATA PROTECTION IMPACT ASSESSMENT RISK ASSESSMENT

LB Camden – agency staff fraud project DPIA Part II (risk assessment)

Step 6: Identify and Assess Risks			
Describe source of privacy (data protection, privacy and information security) 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).** Assess risk assuming there are no controls in place-controls/mitigations are discussed in the next step. **Use tables 1, 2 and 3 in the appendix to help you.** *Note that risks and scores are subject to review and change by IRT/DPO* Add in additional rows as necessary.	**Likelihood of harm- see table 1**	**Severity of harm- see table 2**	**Overall risk – see table 3**
1. There is a risk that an external attacker gains access to personal data.	Unlikely	Minor	4
2. There is a risk that information could be lost, released or shared inappropriately.	Unlikely	Minor	4
3. There is a risk that data disclosed are not required for the purposes of fraud detection, or are excessive.	Unlikely	Minor	4
4. There is a risk that data is retained longer than is necessary for the purposes of NFI	Unlikely	Minor	4
5. There is a risk that people will be misidentified as a result of data processing.	Unlikely	Minor	4
6. There is a risk that personal data will be used for purposes other than those intended.	Unlikely	Minor	4
7. There is a risk that a data subject is not informed about the use of their personal data	Unlikely	Minor	4
8. There is a possibility that a member of the NFI participants staff may seek to cause harm through disclosure of personal information	Unlikely	Minor	4
9. There is a risk that a data subject's data is inaccurate	Possible	Minor	6

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, and not all risks can be eliminated.* Then calculate the risk that remains after the mitigations/controls are in place: the residual risk. Tables 1, 2 and 3 will help with this. *Note that risks and scores are subject to review and change by /DPO* The Information Asset Owner/s need to decide if the mitigations are achievable and if the residual risk is accepted in the 'measure approved?' column by inserting a Yes or No. Table 4 provides guidance on what level of residual risk could be acceptable.				
Risk identified in step 6	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
1. There is a risk that an external attacker gains access to personal data	The contractor, Synectic's who provide the NFI and NFI fraud hub systems has ISO 27001 accreditation. The NFI environment at the supplier is accredited against government standards annually - including penetration testing and IT Health Checks undertaken by specialist 3rd party company. All data transmissions (unless an exception is approved) are via the secure NFI environment.	Reduced	Low	
2. There is a risk that information could be lost, released or shared inappropriately	Controls are per the above	Reduced	Low	
3. There is a risk that data disclosed are not required for the purposes of fraud detection, or are excessive.	The data required from participants will be the data that is adequate, relevant and limited to what is necessary to undertake the matching exercise; to enable the accurate identification of Individuals; to report results of sufficient quality; and to meet the purpose of preventing and detecting fraud.	Reduced	Low	
4. There is a risk that data is retained longer than is necessary for the purposes of NFI	The NFI has published a data deletion schedule. The Data Deletion Schedule applies to the NFI data matching exercises. Our IT contractor provides certificates of deletion. This Data Deletion Schedule covers all proof of concept (research and development) data	Reduced	Low	

	matching unless a specific timetable has been approved and documented as part of the proof-of-concept project scoping.			
5. There is a risk that people will be misidentified as a result of data processing	The Cabinet Office, working with Synectics and participants has built up a robust series of matching rules that aim to identify the same (or different as applicable when carrying out address matching) individual across multiple data sources. NFI participants are informed to check all matches and ensure that ID is certain before taking any action and have regard to sensitive matches such are those to deceased or vulnerable people	Reduced	Low	
6. There is a risk that personal data will be used for purposes other than those intended	Participants' use of the NFI data is governed by the NFI Code of Data matching Practice In addition to this Code, when participating in data matching exercises, bodies should have regard to any other relevant data or information sharing codes and guidance, including any statutory guidance from the Information Commissioner. London Boroughs have clearly set-out the purpose for how the data will be used and it is clear with the NFI team at the Cabinet Office and Synectic's. The Cabinet Office has a Governance Board in place that signs off all data matching including proof of concept work. With a representation from Cabinet Office Legal Services.	Reduced	Low	
7. There is a risk that a data subject is not informed about the use of their personal data	The Cabinet Office Code of Data Matching Practice sets out that participants must comply with data protection legislation. This requires that data must be processed lawfully, fairly, in a transparent manner and for specified and legitimate purposes. In addition, data controllers must inform individuals that their data will be processed. All London NFI Fraud Hub participants are required to complete and agree with their	Reduced	Low	

	respective Information Teams, a DPIA and achieve sign-off. London Boroughs are required to ensure their privacy notices accurately reflect the use of personal data for the detection and prevention of fraud. Participating bodies must provide a written notice, known as a privacy notice, which contains the information required by data protection legislation. Participants must submit a declaration confirming compliance with the privacy notice requirements to the Cabinet Office. The Cabinet Office NFI Team monitor submission of these declarations to ensure they are completed in the required timescale. If the Cabinet Office becomes aware that privacy notice requirements have not been adhered to, it will agree the steps necessary for the participant to achieve compliance. The Cabinet Office may seek input from the Information Commissioner as part of this process. The Cabinet Office has a privacy notice for the NFI. This notice sets out how we will use personal data, and a data subjects rights. It is made under Article 14 of the General Data Protection Regulation (GDPR).			
8. There is a possibility that a member of the NFI participants staff may seek to cause harm through disclosure of personal information	A NFI Security Policy is in place and participants must confirm their compliance. All users should have undergone appropriate pre-employment screening checks to ensure that the threat to the system or the information is mitigated as far as possible. This includes any subcontractors, third parties or temporary staff that will be using the system on behalf of the organisation. It is recommended that the following standard (or equivalent) is adhered to: HMG Baseline Personnel Security Standard.	Reduced	Low	

9. There is a risk that a data subject's data is inaccurate	Once data is received it is quality checked by Synectic's, and, if it is found to be inaccurate, a request will be made for resubmission of that data. We will work with our recruitment agency/managed service provider partners to ensure that data is correct, where this may be found to not be the case. We inform the data subject they have the right to rectification on our privacy notice.	Reduced	Low	
Residual (remaining) risk level when all mitigations have been applied: *Note IRT/DPO may change this*				
Low				

Step 8: Record Data Protection Officer advice and outcome	
DPO involved in preparing DPIA? If not, name of IRO	Sarah Laws, Data Protection Manager
DPO advice	
Information Asset Owner acceptance of residual risks	Joanna Brown, Director of People and Inclusion
This DPIA will kept under review by: *(usually the author or the IAO)*	[redacted], Principal Investigator

Version Control

Version	Reason	Date	Author(s)
1.0	New DPIA	27/10/23	[redacted]

Appendix 1
Risk Assessment Tables

Table 1 Likelihood of Risk Occurring

Rare	One-off failure
Unlikely	Possible that it may reoccur but not likely

Rare	One-off failure
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	Willful 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

Table 4: is the risk level acceptable?

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