Data Protection Impact Assessment (DPIA)

You are advised to refer to the guidance material before completing the form.

Data Protection Impact Assessment (DPIA)	
Project Proposal Name:	Palantir Foundry Platform (Nectar)
Force:	Beds
Department/Area:	SSID - Business Change
Force SPOC:	[redacted]
Information Asset Owner:	
DPIA Advisor:	
Date approved and signed off by Information Asset Owner:	03/02/2025 – [redacted]
Date on which processing will commence:	03/02/2025
Date submitted to Information Governance:	04/07/2025
Date submitted to Information Assurance Unit (if applicable):	04/07/2025
Information Assurance Unit advisor (if applicable):	[redacted]
Note: DPIA Advisor will endeavour to give an **initial response** within 10 working days of receiving the completed form.	

Information Governance use only	
Reference number:	
Date published:	04/07/2025
Information Sharing Agreement required? (if so, please record the date and name of the person contacted).	Y/N
High risk DPIA? If yes, please ensure the DPIA is added to the risk register.	Y/N
Consultation	
Data Protection Information Advisor	[redacted]
Chief Information Asset Owner	
Data Protection Officer (DPO)	
Head of Records Management	
Chief Information Security Officer (CISO)	
Senior Information Risk Owner (SIRO)	

Section 1 - Purpose, Scope and Context

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

Ensure to avoid technical language and acronyms.

1.0 Please give details of the project/process/system.

Palantir Technologies Foundry is a comprehensive data integration and analytics platform designed to help manage, analyse, and derive insights from their data. Key features and capabilities of Foundry:

1. Data Integration: Foundry integrates data from various sources without duplicating the underlying assets, ensuring a single source of truth.
2. Ontology-Powered: The platform uses an ontology to represent the objects, actions, and processes of a business, enabling seamless decision-making and automation.
3. AI and Machine Learning: Foundry supports AI and ML workflows, allowing users to build [redacted]
4. Collaboration: It enhances real-time collaboration between data, analytics, and operational teams, ensuring that insights are actionable and integrated into daily operations.
5. Scalability: The platform is designed to scale with the needs of the enterprise, supporting complex and large-scale data operations.

Foundry is a SaaS (Software as a Service) [redacted]
By design, it meets the needs of the National Cyber Security Centre (NCSC) [redacted] principles. The capability of Foundry is interfaced into a single front-end web-based applications. Data integrations into our core systems to Foundry enables data from various sources to be leveraged into a singular view for an individual to consume, whether it be for information purposes, review, [redacted]. Access will be available by laptops and desktops. This application does not utilize causal AI. It neither makes decisions nor draws inferences. Instead, all data is provided to a human for decision-making

The Ontology-Powered part of the platform will use the data from the data integrations and be re-engineered into platform. Any engineering completed will be done based on requirements. All data surfaced into the platform will be robustly tested and approved by data owners.

[redacted]

[redacted] Each connection will have a different data time refresh rate which is collated in a system list document.

This DPIA is a master DPIA for the use of the Foundry platform within BCH Policing and should sit as a master above the annex DPIAs for each underlying application hosted in the platform. Each application within the Foundry platform will have its own annex DPIA detailing the source systems integrated and the process of that information asset. There is an equality impact assessment completed for the overreaching programme, [redacted]

[redacted]

By implementing a single front-end system, we can:

- Explore the feasibility of write back to source systems to remove process wastage
- Automate data retrieval and processing
- Provide a unified view of data for decision-makers

This approach avoids the need for on-premises data storage or large cloud repositories, reducing costs and ownership challenges [redacted]

Our goal is to enable data sharing regardless of the source system, improving efficiency and decision-making both operationally and strategically.

This implementation of the Foundry Platform is predominantly under Part 3 (Law Enforcement Purposes) of the Data Protection Act (DPA) 2018. However, there will be cases where processing will be for non-law enforcement purposes, UK GDPR will apply as specified in each use case. The primary goal is to help Bedfordshire, Hertfordshire, and Cambridgeshire Police, [redacted] This will develop tools to better protect vulnerable people by preventing, detecting, and investigating crime. The Foundry Platform can identify key patterns and automate tasks, aiding decision-making and creating a more efficient workforce.

1.1 Please explain the aim, purpose and intended effect the project/process/system will have on: the force; the data subject; and the public, including benefits and disadvantages.

Aim and Purpose

The primary aim of the Foundry project is to create a real-time data-sharing network across BCH [redacted] The purpose is to enhance data interoperability, streamline data processes, and improve decision-making capabilities by consolidating various data sources into a single, unified view.

Intended Effects of the Programme

Force –

Benefits:

- Increased Operational Efficiency: Automation of data retrieval and processing minimises manual tasks, enabling personnel to concentrate on high-priority activities.
- Enhanced Informed Decision-Making: Consolidated data views provide in-depth insights, supporting both tactical and strategic decision-making processes.
- Increase System Interoperability: [redacted]
- Increase Scalability and Flexibility: The platform is designed to scale with organisational needs, accommodating complex and large-scale data operations as the organisation grows.
- Disadvantages:
- Complex Implementation: The integration and setup of the system can be intricate and require significant resources.
- Training and Adoption: Effective use of the new system necessitates comprehensive training for officers and staff, which may temporarily divert resources from other activities.

Data Subject –

Benefits:

1. Enhanced Protection: Advanced data analysis capabilities aid in the prevention, detection, and investigation of crimes, thereby safeguarding individuals.
2. Increased Service Efficiency: Accelerated and precise data processing leads to faster responses and improved service delivery.

Disadvantages:

1. Privacy Concerns: Potential issues regarding data privacy and the handling of personal information may arise.

[redacted]

Public Impact –

Benefits:

1. Increased Community Safety: Enhanced crime prevention and investigation capabilities contribute to safer communities.
2. Improved Transparency and Trust: Effective data management and sharing practices can build public trust in law enforcement agencies.
3. Improved Resource Optimisation: Efficient resource utilisation can lead to better public services and reduced operational costs.

Disadvantages:

1. Public Perception Issues: There may be skepticism or resistance from the public regarding data sharing and privacy concerns.

[redacted]

Summary

Overall, the project aims to significantly enhance the capabilities of the police force, improve the protection and service to individuals, and benefit the public through increased safety and efficiency. However, it also brings challenges related to [redacted] privacy, and public perception that need to be carefully managed. A communications plan will be developed and delivered to ensure all stakeholders are communicated with appropriately. Similarly, each Nectar Project will detail a full benefit realisation plan.

1.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

Categories of personal data used will vary for each use case for both projects. However, the Foundry platform will require and be used to access personal information which will include personal and special category data.

1.3 Will special category data be used in the proposal? (Select all that apply)

[redacted]

1.4 Will it involve the collection of added information about individuals? Will the Force collect data that it has not previously collected or had access to?

☐ Yes
☒ No

If yes, please give details.

1.5 How many individuals will the processing affect? (Please specify one answer below)

☐ Fewer than 100 data subjects
☐ 100 to 1000 data subjects
☐ 1000 to 5000 data subjects
☒ More than 5000 data subjects

1.6 What categories of data subject are involved? (Please select all applicable categories below)

[redacted]

[redacted]

☐ Other

If other, then please provide further details below:

Click here to enter text.

1.7 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?

For example, can the aim be achieved by using less data or different types of data?

Are all categories of data necessary to achieve the aim?

Using personal data is necessary to achieve the aim of enhancing crime prevention, detection, and investigation, as well as, enhancing operational and organisational intelligence for several reasons:

Necessity of Using Personal Data

1. Accuracy and Relevance: [redacted]
2. Contextual Insights: Personal data helps in understanding the context of incidents, which is essential for effective law enforcement and safeguarding vulnerable individuals.
3. Operational and Organisational Efficiency: Access to comprehensive personal data allows for quicker and more efficient responses, reducing the time needed to gather information from multiple sources.

Alternatives and Data Minimisation

1. Using Less Data: While it is possible to use less data, it may compromise the effectiveness of the system. For instance, anonymised or aggregated data might not provide the detailed insights needed for specific investigations or operational decisions.
2. Different Types of Data: Non-personal data, such as environmental or transactional data, can be useful but often lacks the specificity required for law enforcement purposes. Personal data is necessary to link actions to individuals and understand their behaviors.

Necessity of All Data Categories

1. Comprehensive Coverage: Distinct categories of data [redacted] provide a holistic view that is essential for thorough investigations and decision-making.
2. Specific Use Cases: Each category of data serves specific purposes. For example, [redacted]
3. Data Minimisation Principle: While all categories of data are necessary, the principle of data minimisation is applied to ensure that only the data required for specific purposes is collected

and used.

Both Nectar Project's DPIA's will detail the data specifics in relation to use cases in platform in their annex DPIA.

1.8 Explain how the use of personal data is proportionate to the aim of the proposal. Weigh the advantages of achieving your purpose against disadvantages to data subjects.

- Existing Data: The data already exists within the policing systems and is accessible to officers and staff who have the necessary access control rights. The proposal aims to present this data in a more structured and useful format to improve police officers and staff decision-making.

- Constructive Use: By surfacing the data constructively, officers can make better-informed decisions without any additional disadvantage to the data subjects. The data is already compliant with MoPI data management regulations.

- Lawful Use: The data is used by officers who already have the access rights and privileges for lawful policing purposes. The new system will support these officers in their roles, enhancing their ability to prevent, detect, and investigate crime.

- Data Security: Throughout the process, all data will be processed securely to protect the rights of data subjects. The processing will comply with the Data Protection Act 2018, ensuring that it is lawful, necessary, and proportionate.

- Legal Compliance: The processing of data is justified under the Data Protection Act 2018, specifically for tasks carried out in the public interest or in the exercise of official authority. Special categories of personal data are processed under conditions that ensure substantial public interest and safeguard the rights of data subjects.

The use of personal data in this proposal is proportionate to the aim of improving policing capabilities. The data is already accessible and used for lawful purposes, and the new system will enhance its utility without compromising data security or privacy. The processing is compliant with legal standards, ensuring that it is necessary and proportionate to the public interest goals.

Section 2 - Information Lifecycle

2.0 Diagrams and Tables

Please insert a diagram or table that demonstrates the flow of data within this proposal.

The Data Flows and Access Diagrams are shown below:

1. Data is captured on core existing systems (e.g., Athena or other force systems) as per the current force process – No Change.
2. Data is uploaded from Athena [redacted] – No Change

[redacted]

[redacted]

2.1 Storage

Describe where and how the data will be stored.

Data Storage

[redacted]

Access Control

[redacted]

Data Collection

- Existing Data: Data is already collected within BCH and recorded on existing platforms like Athena, following established policies and governance. No new data is collected within BCH.

Data Transmission

[redacted]

[redacted]

2.2 Use

Describe how the data will be used. Describe whether it involves new technology or novel processing.

Data Usage

- Purpose: The data will be used to populate content in applications developed on the Foundry platform, based on business requirements.

[redacted]

- Enhanced Functionality: The platform provides greater functionality, presenting data in a more digestible and informative way. This allows users to make clear decisions without needing to extract and analyse data separately, thus avoiding duplicate storage.

[redacted]

- Selective Data Retrieval: The system does not harvest all data from the source system but retrieves specific information based on requests. For example, it can connect to all offender details but will only retrieve information related to a specific individual, such as 'John Smith,' when constructing a profile.

Technology and Novel Processing

- Foundry Platform: The technology used is Palantir Foundry, which is not newly developed but is widely used across the UK public sector, including the NHS, Military, and Cabinet Office, as well as European law enforcement.
- Existing Technology: Foundry leverages existing technologies used by BCH, [redacted] and integrates them into a cohesive platform, enhancing data processing and analysis capabilities without introducing novel or untested methods.

2.3 Recording

Describe the processes for recording the data.

Palantir does not capture new data other than what is necessary for auditing system use activity and login information, which is stored in audit logs accessible only through the audit application provided to BCH PSD [redacted]

[redacted]

User Identification

- Access Granting: Ability to identify who granted access to the system and when.
- Access Levels: Ability to identify the access levels granted to each user.
- Permissions Pyramid: Provision of a clear hierarchy of permissions to see proposed user access to different data levels and permissions.

Activity Tracking

- User Actions: Ability to identify specific times, dates, and users for:
  - Viewing a POLE record (or equivalent).
  - Commencing searches.
  - Editing or creating data within the system.
  - Exporting or deleting data within the system.
  - Some navigation within the system (details to be defined upon firsthand use).

Logging and Auditing

- Data Extraction: Ability to extract logging/auditing data from the system.
  - Export data into a CSV file for review in Excel in a workable format as deemed by auditors.
  - Use of an in-built tool, if available, to complete the above.
  - Clear ability to use third-party tools to process this data.

2.5 Processors

Describe the use of processors. If a third party is being used, then is a contract in place to regulate the relationship? Will the data be processed outside of the UK or the EU?

Data Hosting and Processing

[redacted]

Product Metric Logs

[redacted]

[redacted]

Information Security

[redacted]

2.5 Sharing
With which external organisation(s) is the data shared, what data is shared, and why?
Describe any sharing that will occur within Force
Outline any national and international sharing or processing.

External Organisations

- No External Sharing: Data is not shared with any partner or external organisations [redacted]

Internal Force Sharing

- Authorized Access: [redacted] data is shared with individuals who have existing authorisation and access rights based on their positions within the organisation.
- Annex DPIAs: Each Annex DPIA will detail the specific data sharing capabilities for workflows. This ensures that data sharing is controlled and documented.

[redacted]

International Sharing

- No International Sharing: There is no sharing or processing of data outside the UK.

2.6 Review and Retention Describe your plan for review and retention, linking to a retention schedule where appropriate.

Governance Controls:

- Retention rules MOPI 1,2 & 3 and/ or PIRM will be integrated into the platform to automatically retain data only for set periods, ensuring compliance with regulatory requirements.
- Data retention periods will mirror core system retention policies and data. A system spreadsheet will be appendixes that will reference the data refresh rates.

Example Process:

[redacted]

Use Case Specifics:

- Each use case and data from additional systems will have specific storage and retention nuances, detailed in the annex DPIA for that data set.

Data Deletion:

- Foundry settings will allow users with appropriate permissions to delete data directly from the platform. This will not delete data from core systems.
- Regular reviews at checkpoint intervals will ensure that data retained in the platform is appropriate.
    - Before any data goes live on the platform, the project conducts data validation testing as part of user acceptance testing to ensure data integrity. Once in the live environment, users can submit data quality issues through the feedback app. These issues will be reported through the usual internal processes. [redacted]
- Data cannot be repurposed beyond its original consent. [redacted]

Subject Access Requests (SARs):

- Foundry does not change the data from core systems, therefore, existing processes for use of personal data could be followed.

Data Management Tools:

- The platform includes data cataloguing, lineage, and search tools to assist with data management.

Workflow-Specific Retention Policies:

- Workflow-specific retention policies will be in place to manage data created in the platform. For example, in use case one, the gateway incoming demand will have a defined retention policy replicating current policies.

Documentation:

- All policies and procedures for Foundry, including overarching and use case-specific details, will be documented and stored in the Police Corporate Information - Nectar - Palantir Foundry Platform - All Documents.

2.7 Disposal
Describe the process for disposal of data, including when and how.

Instruction-Based Deletion:

[redacted]

Data Formats and Export:

- Data is stored in standard, non-proprietary formats, allowing BCH to export or migrate data according to local security policies and protocol permissions.
- Foundry supports interoperability with other systems using open APIs.

Confidential Information:

- Palantir will return or destroy any confidential information as directed by BCH and in accordance with Palantir's policies, regulatory, and contractual requirements.
- Evidence of destruction is provided through certification.

Sanitisation Methods:

[redacted]

2.8 Audit
If applicable, is the system auditable? Does it have a function to pull reports to audit access/usage of the system?

Yes, the Resource Manager tool is available in the environment to provide auditable user activity tracking. It can generate reports as needed. BCH PSD Audit Specialists have collaborated with Palantir to design and produce a bespoke audit interface for the platform, which is exclusively accessible by BCH PSD/ACU. For BCH PSD, this meets their requirements.

BCH PSD and BCH Information security have access to complete audit capability in the application when required.

[redacted]

Section 3 - Security, Access and Transfers

3.0 What security measures will be in place to protect the data? Describe the physical, organisational, technical security measures that will be in place.

Security measures include a combination of physical, organisational and technical security controls.

Physical Security Measures

[redacted]

Organisational Security Measures

[redacted]

Technical Security Measures

[redacted]

3.1 Access			
Who will have access to the system? e.g. supplier, staff within the force, third parties.	What is the purpose of the access? e.g. carrying out work tasks, supplier needs for troubleshooting purposes	How will they access the data/system? e.g. remote access, individual log in, etc.	What level of data will they have access to? Partial data, all data etc. If partial, please specify.
Officers and Staff employees of Bedfordshire police Hertfordshire Police	Conduct their existing role within the organisation role in law enforcement.	[redacted]	They will have access to the level of data they currently have access to when accessing the

Cambridgeshire Police [redacted]	From collating and researching information or intelligence on a subject. Importing and recording activity withing an operational and strategic service of BCH policing. Each Annex DPIA with specify the specific purpose of access and use	[redacted] This is only accessible through a BCH ICT issued device through dual authentication.	source system using their credentials. The exact data levels here and drawn-out data schemas for connection for each application use case is drawn out in that Annex DPIA.

[redacted]

3.2 Data Transfers

Transferring data outside the UK but within the EU?
☐ Yes
☒ No
If yes, please give details.

Transferring data outside the EU?
☐ Yes
☒ No
If yes, please give details.

3.3 Assets
Please give details of the assets that you intend to use.

Hardware ☒
Software ☒
Networks ☒
Hardcopy/Physical e.g. paper ☐
Other ☐

3.4 External User Access to Police Systems
This section is only applicable if seeking to grant external users access to police systems

Systems List all systems external users will have access to	[redacted]
Users List the job roles and names of those who will have access	
Vetting What vetting level will users require?	
Location What will the location arrangements be? Will access be on a police or non-police site?	

	[redacted]
Equipment Will access be through police equipment? **Frequency** Will frequency of access be stipulated or monitored?	Equipment [redacted]
Limitations What limitations will be placed on how shared information may be used?	The access to hardware, software and data is for the sole purpose of creating applications in foundry. Staff allowing access will sign and agree to security measures listed below.
Security What measures will be in place to ensure appropriate security is afforded? *(e.g., will location be subject to access control, how is data transferred between systems securely)*	[redacted]

[redacted]

Section 4 - Lawful Basis
4.0 Lawful Basis To process personal data, you must have a lawful basis. Please select the one appropriate lawful basis from the drop-down list.
Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes): Necessary for a law enforcement purpose Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes): Necessary for the performance of a task carried out in the public interest or in the exercise of official authority
4.1 Lawful Basis – Special category data If processing special category data, you must have identified a further lawful condition
Operational Data: The processing is strictly necessary (please tick to confirm) ☐ **AND** One of the following conditions applies (select from the list): Safeguarding children and individuals at risk
Administrative Data It is necessary for one of the following conditions (select from the list): Archiving/ Research/ Statistical **OR** It is in the substantial public interest (tick to confirm) ☐ **AND** for the following purpose: Preventing or detecting unlawful acts and protecting the public against dishonesty, malpractice, unfitness or incompetence

Section 5 - Consultation	
You should consider seeking the views of data subjects unless there's good reason not to. If it's not appropriate to consult, then you must clearly document the reasons why. For example, if the processing is taking place without the knowledge of data subjects and consultation would prejudice a law enforcement purpose then you should make this clear. If the processing involves staff data, then you consider consulting them or their representatives.	
5.0 Do you intend to consult data subjects?	
☐ **Yes** If yes, then outline your plan in **Section 5.1** below together with details of consultation with other stakeholders.	
☒ **No** If no, then outline why this is the case in the text box. Once completed, outline whether you will consult any other stakeholders in **Section 5.1** below.	Overarchingly no, however engagement will be made with stakeholders and community members such as victim support groups and partners but not with victims or offenders of crime into their data in this format as we already captured to the storage location and retention of that data in line with existing processes and governance.

	However, should specific consultation for an annex application use case be different than this will be articulated in this Annex DPIA for this application.

5.1 Consultation Action Log
Explain what steps you will take, or have taken, to consult stakeholders. Stakeholders may include:

- Data subjects
- The public
- Union representatives
- Information Assurance
- Information Rights
- Force Legal Services
- Partner agencies
- Data processors
- Information Commissioner's Office (ICO)

Who	When	How	Outcome
Information Rights	On-going	Project Board & meetings	Review of DPIA and consultation with Information Assurance Unit regarding security risks
Information Assurance	On-going	Project Board & meetings	Advice regarding technical security risks posed by foundry and the measures and settings that need to be in place.
Palantir (data processor)	On-going	Project Board & meetings Privacy and Civil Liberties Team	Information regarding vetting of staff, technical information, and assurance around information governance arrangements. Ensuring that the applications are developed with the intention of use of the tool, privacy security and safety of those involved.
Records Management	On-going	Meetings	Advice in Information Management meetings to ensure compliance with retention polices, MOPI and accuracy in Information Asset Owners being identified.

Section 6 - Data Ethics

Data ethics is a branch of ethics that addresses the moral issues relating to data during its phases of processing, creation, sharing, dissemination, generation, recording, and correspondence.

To enable us to comply with the Data Ethics, we must ensure we adhere to the overarching principles and demonstrate:

- Public benefit and user need
- Alignment with relevant legislation and codes of practice
- Data will be proportionate to the user need
- Data will be well defined, and limitations understood
- Working practices will be robust and skilled
- Transparency and accountability
- Responsible use of data

Considerations surrounding the ethical use of data should be a key component of your project to ensure the appropriate and responsible use of data.

If the project/process being proposed requires you to consider data ethics, please complete the following document. Every time the project/process is changed or updated involving personal identifiable data, the document should be updated to reflect your considerations of data ethics and reasoning to move forward and go ahead with the process/use of personal identifiable data.

Please note this document does not need to be shared with Information Governance. It is designed to be managed and updated locally to ensure Data Ethics requirements are adhered to throughout the course of the project.

Section 7 - Full Risk Assessment	
Identify and Assess Risks In this section you must detail all data protection risks, as well as any associated with privacy and the rights and freedoms of individuals. Please see Annex A where you can find the Data Protection Principles which may help you identify risks.	
Examples of **risks to individuals** include: • Discrimination • Identity theft • Financial loss • Reputational damage or embarrassment • Physical harm • Wrongful arrest or prosecution • Loss of confidentiality • Inability to exercise rights Consider the impact on individuals and any harm or damage that might be caused, whether physical, emotional, or material. Different levels of interference may occur at different stages of the information lifecycle. The European Court of Human Rights has held that a public authority merely storing data is a limitation on the human rights of data subjects.	Examples of **corporate risks** include: • Failure to protect the public • Loss of public confidence • Civil litigation • Reputational damage • Regulatory action • Breaching other legal obligations
You should identify **solutions** such as: • Deciding not to collect certain types of data • Reducing the scope of processing • Reducing retention periods	• Restricting access to data • Training staff to understand the risks • Anonymising or pseudonymising the data

• Taking additional technical security measures • Following approved codes of conduct				• Using different technology • Using an alternative third-party processor		
Describe the source of risk and the nature of potential impact on individuals.	**Likelihood of harm**	**Severity of harm**	**Initial Risk Score**	**Mitigation/ Solution**	**Result**	**Residual Risk**
	1 - Remote 2 - Possible 3 - Probable	*1 - Minimal 2 - Significant 3 - Severe*	*High Medium Low*	*Describe the mitigation and whether it will be implemented*	*Is the risk: - Eliminated - Reduced - Accepted*	*High Medium Low*
Data Minimisation Risk that personal data is used for analytical purposes when it is not proportionate or necessary. (s.37 of DPA 2018) It is possible that personal data to be provided may be excessive for the new purpose. [redacted]	3	3	High	Data fields can be chosen so only those relevant and necessary for chosen Application/report in a way to avoid wherever practicable excessive data. No changes to the original investigation data will occur. Access controls for specific user groups at Row and column-based access controls This ensures data is not accessible to officer in foundry that they would not have accessible to them for a policing purpose within the source systems.	Reduced	Medium
Purpose Limitation	3	3	High	This DPIA covers the overarching use of the	Reduced	Low

Risk that the data or tool will then be used for additional purposes not captured in the DPIA. s. 36 (3) b - Processing for the new law enforcement purpose is necessary and proportionate to the original law enforcement purpose.				Application each Annex DPIA will cover an application / use case inside the Nectar Palantir Foundry product and the associated systems / information assets connected to this application and the purpose for this. BCH policing and the governance of this produce will follow a procedures documentation and change requests for the development of any new capabilities of the platform to ensure those changes stay within the agreed parameters or if new documentation is required that documentation is completed in accordance with organisational process.		
Accuracy Information on an individual, needs to be the most up to date information we have on the subject. Therefore, there is a risk that the data held on a subject may not be accurate.	3	3	High	As part of the development of each workflow and application the accuracy of the data will be reviewed. This review will assess whether data presented in reports is correct and consider the limitations around the timeliness/age of the data before deciding regarding roll out. During the development of each flow and application said data application foundry will only be	Reduced	Low

				available to [redacted] and identified test group of officers. External validation of the foundry platforms ontology and the output performance of the platform will be completed with full testing before the live deployment of the foundry platform and that model into an operational or strategic policing setting. The data that is connected into foundry is from [redacted]		

				[redacted]		
Security Unlawful attempts to access and/or compromise the integrity, confidentiality, or availability of the data. Integrity and Confidentiality: (DPA 2018 s40) [redacted]	3	3	High	Auditing, monitoring, and logging have been enabled across the platform Accessed through Resource Management Tool Access control is owned and managed by BCH ICT for people using the system. Foundry's audit logs capture actions and resource requests throughout the platform. This includes, but is not limited to actions to read, create, modify, or delete data; successful and unsuccessful logins and logouts of users; and modifications to accounts (such as adding or deleting a user). These audit log events are attributed to a user, and record the time, date, and action. Foundry's audit logging event coverage and content follows industry best practices and meets the requirements for standards such as NIST 800-531. Foundry's audit logs are available to BCH PSD This allows PSD to monitor the use of	Reduced	Low

				their Foundry instance to ensure that no misuse is taking place.		
Security Data sanitisation and Equipment disposal Storage Limitation: (s.39 of DPA 2018) There is a risk that data might be retained by the processor or sub processor(s) for longer than is necessary for the purpose.	3	3	High	At the end of the contract, Palantir will destroy all data stored in Foundry on the instructions of the BCH Police. Deleted data is sanitised through the destruction of the encryption keys. The Palantir Foundry platform stores data in standard, non-proprietary data formats, BCH can export or migrate data as per local security policies and protocol permissions. Foundry supports interoperability, using open APIs to enable integration with other systems. [redacted]	Reduced	Low

				[redacted]		
Security Risk to data at rest if not subject to necessary encryption.	3	3	High	All customer data in Foundry is encrypted, both in transit and at rest. This encryption is enabled by default and cannot be turned off. [redacted]	Reduced	Low
Data Subject Rights Risk that personal data within applications or reports is extracted and not managed in a way that allows data subject's rights (access to their data, right to rectify inaccurate data).	3	3	High	Data created will be managed centrally. Accurate records in the ROPA against source systems will require what columns and rows of data are being exported. To foundry in addition to sentinel reports.	Eliminated	
Data Sharing:	3	3	High	Palantir will sign an undertaking	Reduced	Low

Data will be viewed by third party Palantir when they are engineering applications. Risk that they will see sensitive personal data that is not relevant. Or that they do not keep the data they should be seeing confidential.				of confidentiality. In addition to a further document for the management of HR information, detailed in these annex DPIA's Palantir staff will when building and engineering the platform have viewable access to policing data when working alongside end users in the business area, engineers are all vetted appropriately. However, when accessing the foundry platform to build and configure they will only have access to the ontology which says what type of data is flowing through not the row detail of that data. There is no storing of data relating to the platform outside of the platform when engineering it. There are no versions or builds held locally. Additionally, as above the appropriate vetting of the Palantir staff will be in place before access is granted.		
[redacted] [redacted] This includes all data that customers decide to ingest into the platform, and any downstream datasets that are derived using that data. [redacted]	2	1	LOW	[redacted]		

protective monitoring purposes, which potentially contain personal data relating to the users and usage of Foundry but do not contain the customer's data stored within the platform.				[redacted]		

				[redacted]		
The nature and breadth of the processing will result in a risk to the rights and freedoms of individuals.	1	1	Low	Access to system is restricted to authorised officers and staff using their authentication controls and 3 support resources from Palantir who have been vetted. Cases and individuals are processed when there is policing purpose to do so in the investigation, prevention and detection of crime or safeguarding of vulnerable persons, where currently that process is conducted through a manual collection and review of data. Although the foundry platform agent connected to source data will review this when reaching out for data, only data associated with the pole request or operation will be processed into the platform to minimise the processing of data that is not required or associated to ensure processing is only conducted for a lawful purpose.	Eliminated	

- Lawfulness: (s.35 of DPA 2018) The processing of personal data is for a Law Enforcement purpose. It is possible for the suppliers to process the data in different ways or demonstrate some insight without access to personal data. The sensitive processing is strictly necessary for the law enforcement purpose and meets a condition in Schedule 8 and the Controller has an appropriate policy document in place.	3	3	High	The Security Operating Procedures, Security Aspects Letter and Data Processing Contract make it clear that the data must only be processed for a Law Enforcement Purpose and that there are civil, reputational, and potentially criminal sanctions if the policy is not followed.	Reduced	Medium
Risk to [redacted] data could be breached in any way through the platform	1	3	Medium	[redacted] that will be connected to the platform is [redacted] However, as this data is provided form a connect to the [redacted] as per the agreements with the consortium on [redacted] this data then falls as BCH data under the BCH ownership and Information Asset Owner. Making this now BCH data, all being containing data about [redacted]	Reduced	Low

				[redacted] Locally BCH will hold the controls to disable the platform and delete all data within the platform / disconnect the platform from the BCH environment instantly should it be required		

Where risks are identified you must take steps to integrate solutions into the project and this must be recorded. If any **residual risks are 'high'** then the ICO must be consulted prior to processing commencing. Examples of risk factors are provided at the top of each section – these examples are a starting point, and you must ensure that all factors relevant to your proposal are considered. If you run out of space, then insert new lines into the table. When completing each section, if you are unable to identify a risk relevant to your proposal then please state "**No risks identified**".

Annex A

Data Protection Principles

1. Fair and Lawful
- Do you need to create or amend a privacy notice?
- If processing based on consent, how will this be collected and recorded?

2. Purpose Limitation
- Does the processing achieve your purpose?
- Will the data be used for another purpose?
- How will you prevent function creep?

3. Data Minimisation
- Will you only process the data needed for your purpose?
- How will you ensure and maintain data quality?

4. Accuracy
- How will you ensure data can be corrected or amended?
- Will you ensure data is accurate and up to date?

5. Retention
- Do you have a review, retention and disposal policy?
- Can data be deleted/erased from all Force systems if required?
- Is the retention period necessary and proportionate?

6. Security
- What technical and organisational measures are in place to protect data?
- How will you protect against unauthorised access, alteration or removal of data?
- What training and guidance will be given to staff?
- How would you identify and manage a breach?
- How will systems be tested?

7. Data Subject Rights
- If an individual wishes to exercise their rights, including requesting access to data, or asking for data to be corrected, amended, restricted or deleted then you must have procedures in place to recognise such a request and refer it to Information Rights.