Data Protection Impact Assessment (DPIA) Screening Checklist & Template

Police National Database

Preamble

The NPCC, as a Controller, is required to comply with Data Protection legislation – (i) the Data Protection Act 2018 (DPA) when it processes personal data for any of the Law Enforcement Purposes, and (ii) the UK GDPR, as supplemented by the DPA, when the processing is for General Purposes (anything that does not fall under the Law Enforcement Purposes definition).

One of the obligations arising from the Data Protection legislation is the requirement for the NPCC to conduct a Data Protection Impact Assessment (DPIA) where the prospective processing of personal data is likely to result in a '**high risk to the rights and freedoms of individuals**'.

Even if that 'high risk' threshold is not reached, the NPCC's position is that it is good practice to complete a DPIA, particularly when developing a Data Sharing Agreement.

The DPIA must be undertaken prior to the processing starting and, in some cases, cannot commence without the prior authorisation from the Information Commissioner's Office (ICO) once they have reviewed the DPIA

The relevant parts of the Data Protection legislation concerning DPIAs can be found at:

- Section 64 of the DPA and Section 65 of the DPA for processing for Law Enforcement Purposes; and,
- Article 35 of the UK GDPR and Article 36 of the UK GDPR for processing for General Purposes.

The ICO has produced extensive guidance on DPIAs for processing for Law Enforcement Purposes and General Processes.

Screening

In order to determine whether a DPIA is required it is necessary to first conduct a screening exercise to assess whether the prospective processing of personal data is likely to result in a 'high risk to the rights and freedoms of individuals'.

The screening should occur where there is any new or significant changes to existing processing of personal data.

Even if the screening does not result in a requirement to conduct a DPIA it is often beneficial to conduct one.

A DPIA Screening Checklist appears on the next page which should be used to determine if a DPIA is required.

DPIA Screening Checklist

If you intend to process any types of the personal data set out in List 1 **and** the processing appears in List 2 a DPIA must be conducted.

List 1 **Types of Personal Data processed**	**List 2** **Types of high-risk Processing**
Racial or ethnic origin	Innovative use or new technology or solutions
Political opinions	Denial of service or rights
Religious or philosophical beliefs	Large-scale profiling, evaluation or scoring
Trade union membership	Biometrics or genetic data
Genetic data	Automated decision-making
Biometric data	Combining or matching datasets
Health data	Invisible processing
Sex life	Tracking or monitoring
Sexual orientation	Targeting of children or other vulnerable individuals
Criminal activity	Risk of physical or mental harm
Allegations	
Investigations	
Proceedings	

Confirm which (if any) of the above apply:

Racial or ethnic origin, biometric data, sexual orientation, criminal activity, allegations investigations, proceedings innovative use or new technology or solutions, combining or matching datasets, targeting of children or other vulnerable individuals, risk of physical or mental harm

Screening undertaken by: **NPCC PND Business Development Manager**

Date undertaken: 26th June 2023

Outcome of Screening:

DPIA required

If the Screening Checklist identifies a requirement to undertake a DPIA (or you choose to undertake one) please move on to the next page. If there is no requirement, please email this document with the fields above completed to dpo@npcc.police.uk

NPCC DPIA Template

The template, starting on the next page, has been derived from the ICO's and can be completed to record details of the DPIA process and outcome.

Steps 1 to 5 and parts of 7 should be completed by an appropriate person with the necessary knowledge of the processing of personal data being considered (normally the Business Subject Matter Expert (SME) and/or Business Lead[1]).

The NPCC DPO will assist completion of the template where required and in any case will complete Step 6 and parts of Step 7.

The fields requiring completion can readily be identified through appearing with a pale blue/green background when a cursor is hovered over them.

[1] Business Lead is likely to be the Portfolio Lead or Head of National Unit. Subordinates with necessary knowledge and authorisation can participate in the completion of this document

Data Protection Impact Assessment (DPIA) Police National Database

Freedom of Information Act & Information Security

This document (including attachments and appendices) may be subject to an FOI request and the NPCC FOI Officer & Decision Maker will consult with the author on receipt of a request prior to any disclosure. For external Public Authorities in receipt of an FOI request concerning this document, please consult with npcc.foi.request@npfdu.police.uk.

In compliance with the Government's Security Policy Framework's (SPF) mandatory requirements, please ensure any onsite printing is supervised, and storage and security of papers are in compliance with the SPF. Dissemination or further distribution of this document is strictly on a need-to-know basis and in compliance with other security controls and legislative obligations.

Purpose

This DPIA document has been used to:

- identify any privacy or information risks concerning the processing of personal data
- determine any mitigations necessary to bring those risks down to an acceptable level
- provide a record of those mitigations and the decision by Business Lead whether to accept and adopt them
- provide a record of the NPCC's Data Protection Officer's views on the initiative.

Document Administration

Government Security Classification:	**OFFICIAL**
If OFFICIAL-SENSITIVE set out any handling instructions below:	
Not Applicable.	
For inclusion in FOI Publication Scheme?	**Yes**
Version:	**8**
Author(s):	**NPCC PND Business Development Manager**

Date Issued: **28th November 2025**

Date to be next reviewed: 1st May 2026

Information Asset Owner (IAO) for this document: **NPCC PND Lead**

Leads' Details

NPCC Coordination Committee overseeing initiative:

Intelligence

NPCC Portfolio overseeing initiative:

NPCC PND Portfolio.

National Unit overseeing initiative:

Not Applicable.

Business Lead for initiative:

NPCC Staff Officer to NPCC PND lead and PND Manager

Information Asset Owner(s) for information involved in this initiative:

NPCC PND lead

Business SME(s) involved in creation of this DPIA:

PND Manager

NPCC Data Protection Officer

Home Office data protection policy advisor

Home Office PND program

Service providers

NPCC PND Portfolio team

Data Protection Advisor:

NPCC Data Protection Officer

Comments:

Not Applicable

Step 1: Introduction

This section is intended to provide a concise introduction to the initiative, how it arose and the processing of personal data it involves.

1a. Provide a short introductory summary of the intended processing, including the purpose(s) of the processing and the desired outcome of the processing.

The Police National Database (PND) provides a national system to share intelligence and information to improve how police forces, law enforcement agencies and other partners work together to safeguard vulnerable people, prevent and detect crime and protect communities from harm.

As part of the duty of accountability and to consider proportionality, the lead controller has considered it appropriate to complete a DPIA for the existing PND system.

The purpose of the processing is to achieve the strategic aims of the PND which have been previously defined as.

- Protecting children and vulnerable people, by being better able to understand the risk they are facing, and by more thorough vetting of people in positions of responsibility and trust.
- Understanding the threat posed by terrorism of whatever nature and helping to reduce the risk of terrorist activity.
- Disrupting and preventing major, serious and organised crime, helping to reduce the harm caused by the most dangerous offenders.

The desired outcome is to provide a secure, accessible national system which effectively shares intelligence across policing and Law enforcement to enhance operational decision making and reduce threat, risk and harm.

1b. Describe where the intention for the processing arose from i.e. who decided to progress this initiative, in response to what?

The Police National Database was established following the tragic murders in 2002 of Holly Wells and Jessica Chapman. The consequent Bichard Enquiry (2004) identified several critical points of failure.

One of these was the inability of police and law enforcement partners to make fully informed decisions on threat, risk, and harm, as they lacked direct access to pertinent information that existed on source systems outside of their geographic jurisdiction. A recommendation was made for a national police intelligence system that provides a national view of the 45 UK regional forces information; this was launched in Apr 2011 (PND).

1c. Confirm whether the processing is for Law Enforcement Purposes or General Purposes. (within policing if the processing is not for Law Enforcement Purposes it will be for General Purposes). Processing could be for both Law Enforcement and General Purposes.

Data will be mainly processed for law enforcement purposes, although general processing will also apply.

PND will be used for law enforcement purposes defined as:

- the prevention, investigation, detection, or prosecution of criminal offences
- the prosecution of criminal offences or the execution of criminal offences
- the prevention of threats to the public (safeguarding)
- the prevention of threats to public security

Whilst PND is a system largely operated within the scope of Part 3 DPA, some processing purposes will be under the provisions of the Part 2 DPA.

- to meet contractual obligations entered by the individual
- to comply with the Controllers' legal obligations
- to protect individual's vital interests
- for tasks performed in the public interest or exercise of authority vested in the Controller
- in circumstances of significant public interest and for the purposes of public safety
- for purposes of police vetting
- missing people and safeguarding investigations where no crimes are suspected

In certain circumstances, data processed initially under Part 2 DPA may, at a later stage and upon evidence, become necessary for a law enforcement purpose. For example, as an investigation develops after the initial report of a missing person.

1d. If relevant, describe what non-Data Protection legislative framework supports or requires the processing i.e. is the processing mandated or required by an Act of Parliament?

The processing is required because it allows the controllers to discharge their core or statutory duties of protecting the public by detecting and preventing crime.

For Police Forces, this duty is established in common law (precedents set by decisions of the courts) and the police have both common law and legislative powers to execute it.

Police powers can be grouped into three categories:

• Powers to investigate crime. This includes a range of powers to collect evidence needed to identify suspects and support their fair and effective trial.

• Powers to prevent crime. This includes a range of powers to maintain public order, prevent anti-social behavior and manage known offenders/ suspects.

• Powers to 'dispose' of criminal cases. These powers allow police officers to dispose of criminal cases outside of court or charge suspects so they can be prosecuted.

Carrying out those core duties requires the police to share information to protect the public from dangerous offenders who travel across police geographic boundaries.

Most of the processing takes place under common law but minimal processing will be under specific law. One example is the power to take an image of an arrested person which comes from Section 64A or the Police and Criminal Evidence Act. Section 64A(4)(a) states that a photograph:

> 'May be used by, or disclosed to, any person for any purpose related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution or to the enforcement of a sentence.'

Non-Police law enforcement agencies will have their powers and purpose from Statutory law.

The Police National Database is one of the mechanisms which allows controllers to share information and thus discharge their Common Law and Statutory duties more effectively.

Step 2: Describe the processing

This section is intended to provide details of the personal data involved and how it will be processed throughout its lifecycle.

Processing Operations

2a. Describe how the personal data involved will be obtained or created, including from where, by whom, by what means, when, and how frequently.

The PND aggregates data from Law enforcement agencies, including the 43 territorial police forces of England and Wales, British Transport Police, Civil Nuclear Constabulary and Ministry of Defence Police, National Crime Agency, Police Scotland, Police Service of Northern Ireland, Royal Military Police and States of Jersey Police.

Data is collected by:

- daily automatic upload from source systems
- direct entry by users with the appropriate Role Based Access Code (RBAC). This is used to collect and link data on groups involved in organised crime, modern slavery, human trafficking and county lines.

2b. **Once the personal data has been obtained set out in chronological order and stage-by-stage how it will be subsequently processed. For each stage describe the processing operation involved, including what will occur, who will be involved, when and how frequently it will occur. Processing will include storage, amendment, disclosure, sharing and disposal of the personal data.**

Stage 1 – Upload

Data is collected by:

- uploads from source systems
- direct entry by users with the appropriate Role Based Access Code (RBAC). This is used to collect and link data on groups involved in organised crime, modern slavery, human trafficking, and county lines.

Data upload is managed by the Home Office through an accredited data load management service provider to ensure data meets the expectations of data quality and those involved in the process. The data load management service provider works with Police Forces and Law Enforcement agencies to establish an effective and secure data feed into the PND.

Before data is allowed to be submitted on an automated basis to PND it goes through four gateways which involve data quality checks to ensure it's appropriate, proportionate, legal and technically fit for purpose. Once the data has been sent to PND, data providers undergo regular Data Quality assessments and are provided with Data Quality Dashboards.

The data load service provider ensures the inbound information is not corrupted, infected, sent in error or sent out of order. Information that fails the validation rules is returned to the data provider for correction.

Stage 2 – Storage

Data is stored in the PND database maintained by a service provider with Home Office oversight.

PND is hosted on servers at secure UK based data centers.

The UK based service provider is ISO 27001 approved with access limited only to approved, security cleared personnel on a case by case basis. They are subject to the security protocols mandated by Police Digital Services, (PDS).

Data uploaded to PND from data providers are stored within folders in their own dedicated environments and are periodically removed. The access to these folders and files is managed by forces according to their information security policies and role based access control. The data provider is responsible for protective monitoring, access control and audit for the environment in compliance with the PDS approved connection method.

Step 3 – Sharing

PND is a searchable database providing services to trained and authorised users, providing current and joined up intelligence, on-demand and at the point of need.

Approved Police Forces and Law enforcement agencies make use of a wide variety of search functions within the PND to collect, assess and share data to support their law enforcement and policing purposes.

Data is shared by the controllers with each other (under the terms of a joint controller arrangement or data sharing agreements). Data may also be shared by the controllers with other organisations which are not joint controllers under the terms of data sharing agreements.

Step 4 – Amendment, review and deletion

Data in PND will be deleted or amended in the following way:

- Automatically – PND is a mirror of source systems. When a record is deleted from a source system, it is automatically deleted from PND when the next data upload is sent for the source system. Only the system belonging to the data source can have records deleted from PND.
- Directly - Records that have been created by Direct Data Entry, (DDE) e.g. Organised Crime Group data, can be manually removed by the owner of that data.
- Weeding - PND has an automatic previous version removal process that applies to all record types except for person records e.g., where a Crime has been submitted to PND with subsequent updates to it, the principle is that the most recent version of the crime is the most accurate thus previous versions can be removed after a prescribed period.

Controllers of the source systems are required to set their data management policies in compliance with appropriate legislation, codes of practice or other relevant policies .

DDE data has a review date set by the user, (maximum 6 years), under police information management rules. One month before the set review date a notification will be sent to the user group that created the record, triggering the review. If the record is not reviewed by the set date it is automatically deleted.

Any non-police agency must complete a Data Sharing Agreement (DSA) outlining their rules for retention review and deletion, they will also have to agree to the principles of the PND codes of practice and the directions within the manual of guidance.

2c. Confirm whether any of the processing will involve joint controllership with another controller(s). If so, describe when and how the personal data becomes subject of joint controllership.

Data within the PND is processed from Law Enforcement Agencies and the territorial police forces of the United Kingdom who all share data with each other, through the PND. A joint controllers agreement exists for the Police Forces and agencies who process data within PND and are members of the National Police Chiefs Council, NPCC. Within the NPCC Joint Controllers' Agreement, JCA, the NPCC PND lead is the 'Lead Controller'.

Data sharing agreements are used for agencies who process data in the PND but are not joint controllers within the NPCC agreement.

2d. **Confirm whether or not any of the processing will involve the use of a processor to process personal data on behalf of the NPCC. If so, describe when and how the personal data becomes subject of processing by a processor.**

On behalf of the NPCC, The Home Office PND Program and a service provider are responsible for the live service and the continuous development of the database.

The Home Office employ service providers to process the data within PND. Data is the subject of processing by the processors when it is uploaded from source systems into the PND.

Data continues to be processed by the processors whilst it remains within PND and until it is amended or deleted by the source system.

A data processing agreement exists between the NPCC PND Lead Controller and the Home Office. Within this agreement service providers are sub processors on behalf of the Home Office.

The NPCC PND lead chairs a quarterly PND National Steering Group which provides governance and oversight for data protection agreements and issues. Data protection documents are held by the Lead Controller.

2e. Describe the extent to which there is likely to be public, media or pressure group concerns over the processing.

Concern could be raised over the volume of data processed in PND, the use of searching facial images and the management of data.

PND holds 5.8 billion searchable records and public concern could be raised regarding security and access to this volume of data.

Retrospective Facial Searching

The Police National Database (PND) does not provide Live Facial Recognition, (LFR), or Operator Initiated Facial Recognition, (OIFR), but it does provide Retrospective Facial Recognition, (RFR), using the facial search function.

The facial search function within the PND provides investigators with an opportunity to promptly identify unknown individuals who are a risk to the public, have committed a criminal offence or are at risk of harm.

It is an effective aid for investigators, helping to safeguard victims, improving the timeliness of investigations and preventing further offending.

The PND Facial Search must only be used where there is a lawful policing purpose, which is defined as:

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility of the police arising from common or statute law

The use of the PND and any data obtained from it must comply with the principles of the Human Rights Act 1998 and be:

- Lawful
- Proportionate
- Necessary

The facial search function is used after a crime or incident has happened, providing investigators an opportunity to promptly identify unknown individuals who are a risk to the public, are vulnerable and or have committed a criminal offence.

Early use of the facial search function can improve the timeliness of investigations by helping investigators to promptly identify suspects and people at risk of harm. This improves the service provided to victims by reducing the time it takes to investigate their crime.

Post-event use of retrospective facial searching compares still images, (probe images), of unknown people against a reference image held within the PND. The probe image could originate from CCTV from a crime scene, social media, video doorbells or other media devices which capture images of suspects.

Reference images are images which are legally collected by police forces, digitally stored and are uploaded to the PND. Facial images collected for people in police custody every time there is power under Section 64A of the Police and Criminal Evidence Act 1984. The PND facial search function can provide an investigator with key intelligence which after further assessment, enquiries and considerations could lead to the prompt arrest of a suspect.

Without this technology investigators would have to rely upon internal police circulations and/or the public to identify unknown suspects from images taken at or near crime scenes.

This increases the time it can take to identify and arrest dangerous individuals but on occasion can also increase the risk to people.

This can happen when images of potential suspects are released to the public and they are misidentified. This could lead to a person or persons being targeted physically or through social media.

Reference images are uploaded into PND from Police Forces custody databases using a daily automated process. When an image is deleted from a source system it is deleted from the PND within 24 hours.

The PND Facial Search facility enables users to upload a probe image into the PND and search across all reference images stored within the PND. The PND user receives a set of possible matches at the completion of the search.

The PND does not provide confirmation that a probe image exactly matches a reference image stored within PND. Only possible matches are provided and the results cannot be used as evidence of identification.

Each facial image, (probe or custody image), is analysed by software when it is uploaded into the PND.

Key points on the face are pinpointed (such as the eyes, ears, nose, and chin) are allocated numerical values.

When a PND user initiates a facial search, the algorithm uses numerical values to assess and measure the separation of facial features in the probe and reference images.

As the algorithm uses and recognises numerical values, not visible differences, people who look different can be returned as 'possible matches.'

Trained PND users and investigators visually compare the possible matches to establish if any of results could be the person in the probe image. Visual checks are a requirement to remove any images of people who are clearly not the person in the probe image.

If a PND user or an investigator believes the possible matches contain an image which may identify the person in the probe image, they will complete further assessments and consider other reasonable enquiries before any positive action is taken. These further assessments could include researching other intelligence, information gained from the scene of a crime, the victim or witnesses or completing further enquiries which could prove or disprove a person's involvement in a crime.

Facial search results are handled as intelligence, not evidence of identification. This is why they are assessed alongside other known information, intelligence or other reasonable enquiries before the person in the image is considered suitable for arrest, interview or other police action.

As a post event tactic, facial search is used as an aid within considered investigations or incidents. Technology does not solely influence operational decisions, trained officers and staff make operational decisions which may lead to an arrest of a person.

Police Forces have developed processes which manage and co-ordinate the facial search function within a department, team and or through trained PND users.

National Guidance and Codes of Practice inform Police Forces on how to manage and use the facial search function with the PND.

PND users can only access the PND if they have successfully completed training and have the appropriate vetting level. Each search on the PND must be justified based on the needs of the investigation or policing operation.

Initial and refresher training is provided by the College of Policing, supported by Police Forces.

The numbers of users who have access to PND is restricted as it uses a licensed model. Licenses are managed and allocated to a person based on a person's role and operational responsibilities.

The PND cannot be directly accessed by every police officer or member of police staff, it can only be accessed through trained staff and officers who have been an assigned a licence based on their role.

The PND is led by a Chief Constable who is the National Police Chief Constable, (NPCC) PND lead. They lead the national governance and work with a PND Senior Responsible Officer from the Home Office and Law enforcement Facial Recognition leads to ensure the PND is used appropriately.

Oversight of the appropriate use of PND facial search is completed through the National Steering Group informed by internal auditing and monitoring of Police Forces.

The Home Office Custody Image Review (written in response to the RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department [2012] in which the courts found that retaining images for non-convicted individuals was unlawful) stated that police forces in England and Wales should review custody images under the rules set out in Management of Police Information.

The College of Policing Authorised Professional Practice for Police Information and Records Management provides police forces in England and Wales direction on the use and retention of Police records. Policing.

The PND processes data from source systems, with reliance on the controllers of the source system to ensure an appropriate data management policy is applied.

The facial search algorithm used within the PND has been tested for accuracy and racial bias in November 2021 and September 2024, a copy of the reports and responses can be found at risk IR32. The results from the Home Office test in November 2021 showed that the algorithm was more accurate at identifying individuals, including those with protected characteristics, than the previous algorithm. The test also showed false positive ethnicity matches decreasing by over 70%,

In September 2024 the National Physical Laboratory (NPL) provided independent equitability testing of the facial algorithm used to search the Police National Database. The test identified bias towards three protected characteristics at the settings currently used.

The response to the independent equality testing can be found at risk IR32.

Due to special category data being used within facial searching an Appropriate Policy Document, APD, has been completed. The APD contains information specifically for the processing of facial searching.

The PND does not currently use Artificial Intelligence, however future development of technology may change data processing. The DPIA will remain under review and will be updated if technical development should be described within this section.

Technical developments will be shared with controllers as part of the change process, this will provide an opportunity to engage with appropriate legal bodies in Scotland, Northen Ireland or The State of Jersey.

2f. Identify which, if any, of the processing operations could potentially present high risks to the confidentiality of the personal data involved.

Evaluation or scoring

PND data can be used indirectly to identify patterns in the data as well as providing statistical data. This can be used by strategic decision makers to draw inferences, enabling effective operational and policy decisions to be made. Data could relate to an individual's economic situation, health, location or movements.

Sensitive data or data of a highly personal nature

PND will hold large amounts of sensitive data, including facial images. This type of data increases the risk to the rights and freedoms of individuals if misappropriated, damage could be done to a person's reputation or other freedoms they are entitled to enjoy within their private life.

Data processed on a large scale

Data on PND will be processed on a large scale. Typically, there has been an average of 1.2 million transactions completed per month by both policing and non-police organisations. This amounts to nearly 13 to 14 million PND transactions a year. In 2023 PND holds 5.8 billion searchable records which will increase as more agencies onboard to PND.

Matching or combining datasets

PND will be combining existing datasets from multiple sources. PND will combine data originating from two or more data processing operations. PND relationships will involve multiple controllers and processors of data which makes it high risk to individuals.

Data concerning vulnerable data subjects

PND will hold data in relation to children, victims, witnesses and vulnerable people.

Innovative use or applying new technological or organisational solutions.

PND will continue to develop and deliver new technological solutions, improving how we search and share intelligence and images.

2g. Describe the extent to which the processing will be novel, new, or not resembling processing previously occurring.

Data processing and the collection of intelligence is under constant review. If new, novel or processing methods are advanced in the future, the DPIA will be updated to reflect the changes.

2h. **Provide an overview of the measures to be put in place to ensure adequate security/maintenance of confidentiality of the personal data when it is processed. These measures may be technical or organizational ones proportionate to the nature of the personal data involved. Technical measures can be defined as the measures and controls afforded to systems, devices, networks and hardware and encompass cybersecurity, encryption and pseudonymisation, physical security, secure disposal, passwords and access controls. Organizational measures may consist of internal policies, organizational methods or standards, and controls and audits. They can include information security policies, business continuity plans, risk assessments, polices & procedures, awareness & training, reviews & audits, and due diligence.**

Technical

PND is hosted in UK based secure data centers with the appropriate level of physical security and its data is classified to Official Sensitive, using the Government Security Classification (GSC). Security operating procedures are in place and PND is subject to regular accreditation and reviews. The processing of data within the PND is within the UK and The State of Jersey

To connect to the PND, vetted users must be authenticated through Identity Access Management (IAM) and be allocated user accounts with the appropriate access only enabled after relevant training.

Attempts to access from an unauthorised network will be rejected and monitored. There is a range of protective monitoring capabilities to detect and respond to suspicious activity.

In August 2023 the Police and Public Protection Technology (PPPT) department within the Home Office provided their assessment against DPA Section 62 system compliance, which concerns the creation of logs that record activity on operation policing databases such as the PND. Their assessment concluded *'PND has been assessed as 'fully compliant', as it meets or exceeds all of the requirements of Section 62'*

The processing of data is reviewed by Police Digital Services in line with national standards. The Police Digital Service are responsible for coordinating, developing, delivering, and managing digital services and solutions that enable UK policing to safely harness technology to improve public safety.

Details on processing are available within the 'PND Business and Technical Guidance'.

Organsiational

Organisations must comply with the security and connection assessments contained within the PND Manual of Guidance. They must ensure PND users successfully complete the appropriate College of Policing PND training courses which cover cyber security, use of police information, personal responsibility and appropriate access. People are unable to access the PND without successfully passing vetting checks and completing the College of Policing training.

Police forces and other law enforcement organisations, processing PND data, are required to comply with detailed security requirements. These are overseen by a national accreditor (from the Police Digital Service), and include provisions for all aspects of security, both physical and technical.

User access to PND data is restricted based on vetting levels and role(s) but also through technical measures provided through IAM.

Access to the data in PND is based on the classification of the information, system criticality and appropriate business need to access the data. Security controls are applied using a risk-based approach, concentrating on protecting the most important data and business activities. All organisations seeking access to PND are required to go through a rigorous assessment process to achieve approval and their use of the system must be necessary and proportionate.

Users are only able to access the type of data and functions based on their vetting and business need. This is delivered through IAM using Role Based Access Controls, (RBAC).

All use of the system is logged and subject to audit.

All activity within the PND is logged; this will include all upload of data, both direct and automatic feeds; searches and other data retrieval; reviews and disposals; and administrative activities.

Audit identifies and prevents misuse and provides learning.

The audit log will be used strictly for the purposes of:

- proving the integrity of the transactional data to support evidential disclosure of fact-based data on PND; and
- monitoring the PND for improper use, including analysing patterns of usage over a period.
- The log will only be available to force auditors, who will only normally be able to see audit data relating to their force. Auditors will carry out both reactive (i.e. investigating where misuse is suspected) and proactive audits (i.e. random sampling of all activities to check for misuse).
- The activities of auditors on PND will also be logged and subject to audit.

Data processing contracts are in place with the Home Office and their data sub processors. The sub processors are service providers contracted by the Home Office to deliver, maintain and develop the PND and manage the processing of data into PND. They are obliged to keep records of all categories of processing activities, including details of:

- the controller and any other processors
- processing categories
- international transfers
- general description of technical and organisational security measures

The PND data load service is accredited by Police Digital Services, PDS.

2i. **If the processing involves use of new or altered software or IT infrastructure describe what measures have been put in place or are planned to ensure that software or IT infrastructure has or will be accredited to confirm it is suitable secure to use.**

The Home Office are responsible for developing and implementing new software or IT infrastructure through the PND program. Key stakeholders within the development or implementation of new software or infrastructure are Police Digital Services, PDS.

The Police Digital Service are responsible for coordinating, developing, delivering, and managing digital services and solutions that enable UK policing to safely harness technology to improve public safety.

PDS review the risk of any developments within the database and work with the Home Office to provide their approval or recommendations before it is used.

2j. Describe the processes that will ensure the personal data will not be retained longer than is necessary for the purposes set out at 1a.

Most of the data is governed by the retention policies within the source systems, as when data is deleted or amended on a source system it will be deleted or amended from the PND at the next automatic upload.

Police forces in England and Wales are required to set their local retention policies in compliance with the Code of Practice on the Police Information and Records Management.

For DDE data the user must set a review date (maximum 6 years). One month before the set review date the PND will send a reminder to the user group that created the record. If the record is not reviewed by the set date it is automatically deleted.

Any non-police agency will have to complete a Data Sharing Agreement (DSA) outlining how they will use the PND and their rules for retention review and deletion, they will also have to agree to follow the principles of Police Information and Records Management, the PND codes of practice and manual of guidance.

Police Forces in Northern Ireland, Scotland or a Crown Dependency will be required to have an appropriate data management policy based on relevant guidance and legislation.

Nature of the Personal Data

2k. Describe the type personal data involved, including whether it is Criminal Offence Data[2], Special Category Data[3], or data subject to Sensitive Processing[4]. Where appropriate list data fields.

The data in PND will include criminal offence, special category data and be subject to sensitive processing.

The following list represents the sets of data that will typically be held on PND:

- names/aliases/nicknames
- address(es)
- date of birth
- place of birth
- sex, gender
- ethnicity/race (codes in development)
- height/physical description
- facial images
- marks & scars (any identifying marks)
- custody record number (taken from the force custody system)
- physical description (including hair colour, eye colour, facial features)
- health information particularly in relation to safeguarding both officers and individuals
- status & identifiers for biometrically processed data held on another database e.g. fingerprints via the IDENT1 system
- employee numbers
- national insurance numbers
- contact details;
- behaviors relating to criminal activity and status within an investigation

The data will also relate to objects, places, events and companies.

PND collates data across 5 key business areas of Crime, Custody, Intelligence, Child Abuse and Domestic Abuse. Intelligence includes modern slavery, county lines, organised crime mapping flagstone records and vulnerable people.

---

[2] Defined where processing is for General Purposes as personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

[3] Defined where processing is for General Purposes as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[4] Defined where processing is for Law Enforcement purposes as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, or of biometric data, for the purpose of uniquely identifying an individual; data concerning health an individual's sex life or sexual orientation.

2l. Describe the volume of personal data involved, including how many individuals it will relate to.

As of 2023, PND contains 5.8 billion searchable records, including 101 million person records, 193 million location records, 186 million object records, 144 million crime records, 128 million markers and 100 million intelligence records.

2m. Describe any criteria used to determine what personal data will be processed.

Data in PND will only be processed for law enforcement purposes defined as:

- the prevention, investigation, detection or prosecution of criminal offences
- the prosecution of criminal offences or the execution of criminal offences
- the prevention of threats to the public (safeguarding)
- the prevention of threats to public security

The criteria used to process data aligns to the Authorised Policing Practice, APP, for Intelligence management and the Code of Practice for the National Intelligence Model.

Data within PND, obtained using the criteria outlined above, may subsequently be used for general purposes e.g. vetting, dealing with missing people.

2n. Describe the measures to be put in place to ensure an excessive amount of personal data is not processed. These may be technical and/or organizational ones.

The information processed in PND is for policing purposes as directed by the PND Codes of practice.

Records are only uploaded to PND from source systems that have a lawful purpose for sharing and the data is aligned to the POLE entities.

Controllers of source systems have privacy notices which details the data being collected and the purposes for which it will be shared.

Business and technical rules are applied to the data loads from source systems to ensure only data which should be processed in PND is uploaded.

Controllers of the source systems which upload data to PND provide training and education to users to ensure data submitted is not excessive.

2o. What measures will be put in place to ensure the personal data processed is of the necessary quality (accurate, complete, clear etc). These may be technical and/or organizational ones.

The PND aggregates data from source systems to provide nationwide intelligence and mapping and searching capability. On connection to the PND it is expected that source systems have their own technical and organisational measures to improve data quality.

Data is collected by:

- upload from source systems
- direct entry by users with the appropriate Role Based Access Code (RBAC). This is used to collect and link data on groups involved in organised crime, modern slavery, human trafficking and county lines.

Data quality in PND is managed through deletion in the following way:

- Automatically – PND is a mirror of force systems. When a record is deleted from a force system, it is automatically deleted from PND. Only the system belonging to that force can have records deleted from PND.
- Directly - Records that have been created by Direct Data Entry e.g., Organised Crime Group data, can be manually removed by the owner of that data.
- Weeding - PND has an automatic previous version removal process that applies to all record types except for person records e.g., where a Crime has been submitted to PND with subsequent updates to it, the principle is that the most recent version of the crime the most accurate thus previous versions can be removed after a prescribed period.

The PND has a PDS accredited load service for authorised data providers which is managed by a service provider commissioned by the Home Office. The load service supports data providers to upload relevant data, whilst performing data quality checks and augmenting their submissions with reference data.

This service checks incoming information and ensures it comes from an authenticated and authorised source, and it meets minimum requirements before accepting it for processing within the PND system.

The information is validated against data quality rules and then stored in the PND. Periodically feedback is given to the data providers in the form of data quality reports and other relevant information.

The load service ensures the inbound information is not corrupted, infected, sent in error or sent out of order. Information that fails the validation rules is returned to the data provider for correction.

The PND Landscape assurance team, work in collaboration with Force and agencies to review and improve the quality of data quality provided by the source systems. This will include reviewing the source systems technical and organizational measures used to manage the quality of their data.

Data Subjects

2p. Describe the types/categories of the data subjects whose data will be processed e.g. victims. witnesses, offenders, suspects, officers, staff etc.

Persons suspected of having committed or being about to commit a criminal offence

Persons convicted of a criminal offence

Persons who are or may be victims of a criminal offence

Witnesses or other persons with information about offences

Children or vulnerable individuals

Police officers or staff (current and former)

2q. Confirm whether the personal data is processed based on data subjects' consent and if so, describe how that consent will be obtained and recorded, and how withdrawals of consent would be managed.

Consent is not used as a lawful basis for processing.

2r. Describe the extent to which the personal data involved will relate to children or other vulnerable people.

Data in PND will relate to children and other vulnerable groups.

PND will allow the creation of records for children under the age of ten for non-offence data, though these instances will largely be for safeguarding reasons.

Audit functions will be used to ensure that access to their data is only permitted where there is a genuine reason to access that data.

PND will maintain separation as much as is possible between suspects and offenders and victims and witnesses.

PND data is distinguishable between personal data based on facts from that which is based on a matter of opinion or assessment. Intelligence reports in PND are evaluated using the 3x5x2 process, as directed within the College of Policing Authorised professional practice for intelligence management.

Both technical and procedural mitigations have been applied to reduce any potential impacts to members of the public.

2s. Describe the nature of the NPCC's relationship with data subjects, including whether they would expect their personal data to be used in this way, and the extent to which they can influence the processing.

The NPCC and the PND will have a relationship with the following data subjects.

Victims of crime, witnesses, people who are suspected of a criminal offence, people who have admitted or been found guilty of a criminal office, police officers and staff.

The groups of data subjects will have differing expectations, as an example people who are victims of crime, or police officers and staff will be aware their data will be processed on police systems but people suspected of criminal offences may not be aware and will be unable to influence its use.

As described in 2q the data controllers of the source systems, Chief Officers for Police Forces, have public privacy notices which explain how people's data will be used and their induvial rights.

Through an NPCC joint controllers' agreement the NPCC PND lead is the controller for PND and acts on behalf of the joint controllers.

Step 3: Consultation

This section is intended to stimulate consideration as to whether the views of internal or external stakeholders should be sought. Initiatives that have the potential to lead to public or media concern may benefit from consultation that could help enhance the processing. Clearly external consultation may be counter-productive if it were to reveal sensitive policing techniques or capabilities. Where the processing is largely consistent with a well-established approach there may be little benefit in consultation.

3a. Describe the extent to which you intend to consult, or already have consulted, with stakeholders on their views of the processing described in response to 2c. Stakeholders can include externally - data subjects, members of the public, campaign groups, partner organizations; internally – information security experts, ethics committees etc.

The PND was implemented following the Bichard Inquiry in 2004 following the conviction of Ian Huntley for the murders of two children, Jessica Chapman and Holly Wells. The inquiry identified it was in the public's interest to improve how police intelligence was shared across England and Wales.

The inquiry and subsequent recommendations were supported by Government, law enforcement and policing.

Recommendation one was to implement an IT system to improve how police intelligence is shared across England and Wales. Following extensive consultation and development, the Home Office delivered the PND in response to recommendation one.

Internal consultation has been completed with key stakeholders within NPCC, Home Office and PND service providers.

3b. If consultation is not intended or is to be limited set out a rationale for adopting that position.

The PND is an established system which operates within a national governance framework, involving numerous stakeholders.

The development and implementation of the PND following the Bichard Inquiry included significant consultation as did the publication of the PND Codes of Practice.

Based on the above no further consultation is intended.

Steps 4 & 5: Identify risks, assess risks, and determine measures to reduce risks

The table overleaf sets out in Column 1 generic information risks that could apply to the processing of personal data under any initiative.

Columns 2 and 3 should be used to record the results of a risk assessment that should be carried out on each potential risk, the numerical result of which should then be added to Column 4.

Once the risk assessment has been conducted the Business Lead for the initiative covered by this DPIA should determine, against their risk appetite, whether the risk should lead to termination of the initiative, or alternatively can be tolerated, or transferred or treated. These terms are described below:

- Terminate - Some risks are so far beyond the tolerance identified by the risk appetite or are assessed as having such a severe impact on the business that the initiative should not be progressed.
- Tolerate – some risks are of a sufficiently low level that no actions need to be taken.
- Transfer – on rare occasions it could be possible to transfer the risk to third-parties.
- Treat – many risks can be treated or mitigated to reduce them to a level that is acceptable to the Business Lead.

Where the decision is to treat the risk the treatment to be applied should be added to Column 7 – Column 6 provides potential risk treatments which can be used as prompts for the completion of Column 7.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	5. Decision (Terminate, Tolerate, Transfer or Treat)	6. Potential Risk Treatment	7. Risk Treatment to be adopted, or comments
Confidentiality-related						
IR1. The information is accessible by people who should not have access to it	**2 Possible**	**3 Severe**	**2 Medium**	**Treat**	Restrict access to the information through appropriate technical, physical or procedural means so that only those with legitimate justification can access it Anonymise or pseudonymise the information where possible	Access to the database is secured through IAMS. Users are only given access when vetted, trained and have been allocated a role aligned to their role. Police Digital Services provide assurance of organistaions security and connection methods. Pro-active audit function is used to monitor use and identify any misuse. Organisations who have access to PND follow procedures as directed by PND codes of practice and manual of guidance. PND has security functions to protect access to data based on induvial users, their roles and the agency. These are explained in more detail within this risk assessment. RBAC – Role Based Access Control – restricts access based on user's role ABAC – Agency Based Access Control – restricts access based on agency. DARC – Data Access Restriction Codes – restricts a user's access based on business need, vetting levels and role. Intelligence uploaded with the PND from source systems will be assessed using the National Intelligence Model. Handling codes will be applied and these will be replicated into PND.
IR2. The system is hosted on an insecure infrastructure or premises. • Insufficient security could lead to unauthorised access internally or externally. This would lead to unauthorised data breaches which could lead to fines by the Information Commission Office (ICO). • There will be a personal impact experienced by the individuals who are subject to the data breach. • Reputational damage would occur within the Police Forces.	**2 Possible**	**3 Severe**	**2 Medium**	**Treat**	The system must be hosted on a secure IT infrastructure, either on police premises or hosted	Database is hosted in UK based servers in secure premises managed by a service provider who is ISO 27001 approved. Provider is subject to the security protocols mandated by PDS. The PND infrastructure is provided by accredited suppliers who are managed by the Home Office and are assessed for their security protocols by PDS. PND is Critical National Infrastructure (CNI) providing additional security support and investment.

IR3. People who should have access to the information have inappropriate levels of access to it	**1 Remote**	**3 Severe**	**2 Medium**	**Treat**	Review technical, physical or procedural measures controlling access to the information on a regular basis and amend where necessary	The most sensitive data within PND has limited access based on the role of the user and their vetting levels. Role based access control (RBAC) is used to ensure users only have access to data appropriate for their vetting levels and role. Data Access Restriction codes (DARC) are also used to manage access to data. **DARC 1** is the default value for information within the PND. It allows sharing of that information within the UK police service and other law enforcement agencies. • All PND users will see headers and records marked as DARC 1 **DARC 2** permits sharing PND information with UK non-prosecuting parties. • All PND users will see headers and records marked as DARC 2 **DARC 3** permits sharing PND information with foreign law enforcement agencies. • All PND users will see headers and records marked as DARC 3 **DARC 4** permits sharing PND Information within the originating service/agency (nationally). • Only users with DARC access level 4 or higher will see a header and/or record marked DARC 4 **DARC 5** permits sharing of PND information with the proviso that the recipient must accept specified handling instructions. Users attempting to access information protected by a DARC 5 value must agree to any attached handling instructions prior to the information being made available by the PND. • Only users with DARC 5 access level will see a record or header marked DARC 5 Users will only gain DARC 4 or 5 access if their vetting levels and role require access. Only a small proportion of users are provided with this access and they are subject to audit. Agency Based Access Controls – ABAC are used when it is not appropriate to share intelligence with an agency and their PND users.

IR4. The information is accidentally disclosed inappropriately	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Educate users on how to prevent accidentally inappropriate disclosure of the information Implement appropriate technical, physical or procedural measures to prevent accidental disclosure of the information	All users of PND have received training and are part of police forces or law enforcement agencies who operate crime and intelligence source systems. Education is provided on inappropriate sharing of information and recording rationales if data is shared. PND users follow the Manual of Guidance which has a section to cover disclosures of data. Data within PND is appropriately marked to ensure the reader is aware of the handling conditions.
IR5. The information is deliberately accessed or disclosed inappropriately	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Educate users on the criminal offences relating to deliberate access or disclosure of personal data (Section 170 Data Protection Act 2018) Educate users on the criminal offences within the Computer Misuse Act 1990 Implement auditing or validation of users' access and/or use of the information	All users of PND have received training and are part of police forces or law enforcement agencies who operate crime and intelligence source systems. Education is provided on the criminal offences relating to deliberate access or disclosure of personal data. PND operates an audit function focused on identifying misuse and logs are maintained for each search completed by users.
IR6. The information is held or used in an insecure environment	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Conduct a risk assessment on the environment and implement appropriate technical, physical or procedural measures to protect the information	PND is accessed through desk based terminal or secure laptops. Desk based terminals will only be in secure premises with appropriate security arrangements for user access (IAM). Secure laptops can only be used when the organisation and the user have agreed to the NPCC Security Operating Procedures (SyOPs) for the Use of Devices Supplying Remote Access to the PND. Key points within the SyOps are. Users who access PND must be aware that they can, where appropriate, access via the SECURE channel or via the PROTECTED channel. Upon completing work on any device, users must ensure that they lock or shut down the device. Users should take care to ensure that they are not overlooked when they are entering their password or when they are working from their device. Should you lose the devices, you must report the loss immediately to the appropriate body in your agency. Internet and e-mail access is disabled whilst on the SECURE channel. Users must not attempt to bypass this to access websites, download applications, etc. Users should always adhere to good cyber-hygiene and should contact local IT/operational security leads for further advice.

IR7. The information can be damaged or inappropriately deleted	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Review technical, physical or procedural measures concerning deletion or amendment of the information on a regular basis and amend them where necessary	Data is deleted from PND through the source systems. Controllers of the source systems are responsible for their review, amend, retain and delete processes. If a record is amended or deleted within a source system it will be amended or deleted in PND, when the next data extract is uploaded to PND. The Home Office uses an accredited service provider to manage data load, data quality and assess the data within PND. If data was damaged or accidentally deleted within PND by a technical issue this would be identified. Measures are in place to prevent and identify data issues; **Prevent Deletes Caused by a person.** All staff are appropriately vetted. Most of the instances of the database they access are read only. Limited people have access to Delete and Drop Table functionality. **Prevent Deletes caused by technical issues.** All code goes through thorough testing. There is a Disaster Recovery site which can be used to reconcile records and recover data. **Identify Data Quality Issues** PND Landscape assurance team conduct surveys to reconcile force numbers against PND numbers. **Identify Deletes caused by technical issues** PND produces logs which are regularly checked and automatic notifications are used to highlight technical issues. The Data Load team regularly checks and reports against potential data quality issues with data loads and record types. During the DMA Gateway process (when Forces/agencies are providing data from a new system), technical reconciliation activity between source system data and data that PND has loaded can identify where deletes have inadvertently occurred.

Integrity-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR8. The integrity of the information is jeopardised	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Review technical, physical or procedural measures concerning the integrity of the information on a regular basis and amend them where necessary	As IR 7 above
Availability-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR9. The information is inaccessible to those who should have access to it	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Review technical, physical or procedural measures controlling access to the information on a regular basis and amend them where necessary	The Home Office manage a 'live service' team who are responsible for ensuring the PND is accessible to users 365 days a year 24 hours a day. PND users can report issues with accessibility to the live service team through the service desk, who are able to assess the risk to the service and prioritise the technical response. If a critical issue is identified, which aligns to the definition of a 'critical incident', the NPCC PND will lead the response working with key stakeholders. A process exists with local administrators to review PND users' levels of access and usage aligned to organizational need.
IR10. The information is not shared when it could be	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Review potential information sharing opportunities and adopt them where appropriate	The Home Office have an onboarding lead and a data load service who are responsible for identifying opportunities or issues with sharing of information from Police Forces or Law enforcement agencies. Members of these teams work with Police Forces and Law enforcement agencies to identify the opportunities/issues and find technical solutions when there is a lawful basis to share data. The NPCC PND lead controller will inform joint controllers and non NPCC controllers of their responsibility to share data, identifying areas for improvement. If the NPCC lead controller identifies an area for improvement, resources are made available to enable a solution. The PND Manual of Guidance provides users direction on the need to share data, especially when managing safeguarding issues. Users of PND and strategic leaders are reminded of the importance of sharing information and the purpose of PND when they are trained, have refreshers inputs or attend CPD events.
IR11. The information is not exploited when it could be	**2 Possible**	**1 Minimal**	**1 Low**	**Tolerate**	Identify and implement other appropriate potential uses of the information	The NPCC PND lead is engaged with other NPCC portfolios to assess and mitigate risk in operational policing.

						The NPCC have a governance framework to enable this engagement and ensure the data in PND is effectively used when there is a lawful basis to do so. Recent examples have engaged the NPCC PND lead to support the prevention coordination committee to provide enhancements to police officer and staff vetting.
IR12. The information cannot be found (e.g. physical documents or searching of IT)	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Ensure the Register of Processing Operations and/or Information Asset Register is completed to record the location of the information Conduct periodic audits to test whether information can be found and undertake any necessary activities to improve the situation	Users of the PND can report any issues with their searches to the live service team through the service desk. This would identify any real time issues with the information being returned on searches. The live service team prioritise their response and would seek to resolve the issues as soon as practicable. A record is maintained of all data loaded into PND and when it is amended or deleted.
Legality-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR13. The purpose(s) for processing the information is unclear	**1 Remote**	**3 Severe**	**2 Medium**	**Treat**	Determine and record the precise reason(s) for processing the information, updating as is necessary	A DPIA has been completed for PND which describes the purposes for processing data within PND. Each Police Force or Law Enforcement agency processing data through the PND must justify their legal position as part of the application process. This will be based on their common law or statutory responsibilities and ensuring they have a policing purpose as directed in the PND codes of practice. The onboarding process will involve legal and data protection stakeholders from the police force, agencies, home office and NPCC. A governance process, led by NPCC PND lead, assesses the lawful basis and purpose for access to PND before authority for access is granted. PND users must state their reason for searches, which is logged and subject to audit.
IR14. There is no lawful basis to process the information	**1 Remote**	**3 Severe**	**2 Medium**	**Treat**	Stop processing the information until a lawful basis for processing it is found Identify, record and regularly review the lawful basis for the processing	As per IR13. If audits identified data from a source system had been processed without lawful basis, the records could be identified and measures put in place to stop further processing

IR15. The information is being used unfairly or without transparency to data subjects	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement physical or procedure measures to ensure transparency requirements are met – including consideration of a Privacy/Transparency Notice(s)	PND data is a direct reflection of data held within the source systems of the NPCC joint controllers or non NPCC controllers. Each controller has a privacy notice which is accessible to the public which explains how personal data will be collected and why it will be shared. The PND was developed to improve data sharing nationally across police forces and law enforcement agencies. The database enables effective data sharing aligned to common law and statutory responsibilities of the controllers and their privacy notices. PND has an NPCC Joint Controllers Agreement, DPIA, and a published Codes of Practice which describes how data is used and when it can be used (law enforcement purposes).
IR16. The information is being used for a purpose incompatible with the reason it was first used/collected	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Document the approved uses that the information may be put to Audit the use of the information to identify any incompatible use, which should be stopped	Controllers who process data from the PND are part of the NPCC joint controllers' agreement or a data sharing agreement which approves the use of the data. The application and authorising process for new agencies onboarding PND ensures the purpose for processing is lawful. PND has an established audit process which reviews users processing and would identify misuse.
IR17. Pseudonymised versions of the information can be altered to identify individuals	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Ensure any pseudonymization information meets the requirements of appropriate published standards	PND regularly uploads data from source systems, accurately reflecting the data stored in the source system. Intelligence and information held in the source systems will have been risk assessed and managed using the National Intelligence Model. PND applies further security measures to restrict access to data (DARC,RBAC,ABAC), to reduce the risk of people accessing data which they should not be able to view. A restricted amount of people have the vetting/access to delete/amend data in PND.
Data Quality-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR18. The information is inaccurate	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement quality assurance processes when the information is first recorded Correct inaccurate data as soon as possible after it is apparent it is inaccurate	The PND has a landscape assurance team who work with Forces and agencies to identify data quality issues. The team complete surveys of the data held in PND and data held in source systems to identify opportunities, areas of improvement and learning. The data load service ensures DQ before it is loaded into PND. They work with Force/Agencies passing their data through several gateways to check/reconcile data. If the data is not of sufficient

						quality, it will not pass the assurance and won't be uploaded to PND. Data Quality and national position on data uploaded is reported monthly and discussed at the PND National Steering Group and Regional User Groups. The NPCC PND team meet with the data load team on a regular basis to discuss data loads, data quality, risks and priorities. The NPCC PND lead will contact Chief Officers and Agency leads when data quality issues are identified and provide resources to improve the issue.
IR19. The information is incomplete	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement quality assurance processes when the information is first recorded	The data load service ensures DQ before it is loaded into PND. They work with Force/Agencies passing their data through several gateways to check/reconcile data. If the data is not of sufficient quality, it will not pass the assurance and won't be uploaded to PND. Source systems controllers are responsible for data quality, and they are supported by the PND landscape team to identify DQ issues and make improvements when required.
IR20. The information cannot be amended when it needs to be	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Adopt processes to append new 'correct' information to the information requiring amendment Implement technical measures to allow the information to be amended	The PND uploads data from source systems, replicating the data in PND. Automated and manual processes exist to ensure that data in PND will be automatically changed, (following an upload from the source system) or manually changed, (through Direct Data Entry)**.** Business and technical guidance exists to explain the processes of upload and the PND manual of guidance provides direction on DDE.
IR21. Duplicate versions of the information exist	**3 Probable**	**2 Significant**	**2 Medium**	**Treat**	Adopt technical and procedural measures to prevent the creation of duplicate copies of the information Run audits to identify duplicate copies of the information Merge the duplicate copies of the information Educate users on the issues arising from duplicated information and the measures they must adopt to prevent the creation of duplicated information	Duplicate records are identified within PND through the measures in place to manage data quality. The DQ measures have been explained in IR 18. When duplicates are identified members of the data load team will work with Force/Agencies to rectify the position. Education is provided to users and controllers regarding the importance of data quality to prevent the creation of duplicate records being uploaded from source systems
Records Management-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments

IR22. Excessive information is held	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Review the scope of the information held and reduce the scope so that it is restricted to that necessary for the purpose it is held Train users on the scope of information that should be collected	The information processed in PND is focused on the scope outlined in this DPIA. Records are only uploaded to PND from source systems that have a lawful purpose for sharing and aligning to the POLE entities. Business and technical guidance is applied to the data loads to ensure the above is followed.
IR23. The information is held longer than is necessary	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Implement review, retention and deletion (RRD) processes (technical and/or non-technical) so that the information is held no longer than is necessary Document the RRD processes Educate users as to their responsibilities in connection with the RRD processes	The PND reviews and deletes records as below. Logs are kept of all deletions and amendments made in the PND. Automatically – PND is a mirror of force systems. When a record is deleted from a force system, it is automatically deleted from PND. Only the system belonging to that force can have records deleted from PND. Directly - Records that have been created by Direct Data Entry e.g., Organised Crime Group data, can be manually removed by the owner of that data. Weeding - PND has an automatic previous version removal process that applies to all record types except for person records e.g., where a Crime has been submitted to PND with subsequent updates to it, the principle is that the most recent version of the crime is the most accurate thus previous versions can be removed after a prescribed period. The PND is a mirror of source systems, the controllers of the source systems are responsible for ensuring they have an appropriate RRD process, following the codes of practice for police information and record management. Police Forces and agencies who process data in the PND agree as part of the onboarding process to follow the RRD process aligned to their source system. The PND landscape assurance team, data load team and NPCC team conduct surveys, audits and training to ensure the importance of data quality is highlighted to users and strategic leaders. The NPCC PND portfolio is pro-actively engaged with other Policing leads to improve how police data is managed and reviewed.
IR24. The information cannot be disposed of when no longer required	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement technical measures to allow the information to be disposed of	As described in IR23 the PND has a stable and effective delete process. If a technical issue was identified, the live service team and the supplier would be aware and would resolve the issue.

Training-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR25. Users of the information are inadequately trained	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement appropriate training for all users	Training for PND users is delivered by the College of Policing and accredited Police Forces. Courses supplied are. PND DDE PND Flagstone DDE PND search user – advance PND search user – basic PND search user – basic and advanced combined PND standard auditor PND train the trainer Users of PND must complete training before they are given access to the database. Additional training is provided for users who require remote secure access. Refresher training is provided through CPD events led by the Home Office or NPCC PND team. The PND National Steering Group core membership includes the College of Policing and the Regional user Groups include local training leads. Training courses can be requested by controllers directly with the College of Policing, through their regional user Groups, through the Home Office or NPCC PND team.
Governance-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR26. There is inadequate policy or procedure surrounding the access or use of the information	**1 Remote**	**3 Severe**	**1 Low**	**Treat**	Implement and maintain necessary policy or procedure concerning the access or use of the information	The PND has a code of practice, a manual of guidance, and business and technical rules which all provide the relevant information to ensure access and use of the data is managed effectively. When new agencies are onboarded to PND, Controllers of source systems will agree to follow the codes of practice, manual of guidance and the other relevant PND policies and practices. Users are trained aligned to Codes of Practice and the manual of Guidance. The NPCC PND team are responsible alongside Home Office colleagues for undertaking reviews of the relevant documents.

IR27. There is an absence of an adequate information sharing agreement (where one is required)	**1 Remote**	**3 Severe**	**1 Low**	**Treat**	Implement and maintain necessary information sharing agreements and review these on at least an annual basis	A Joint Controllers Agreement is agreed by the NPCC Police Forces, Territorial Forces, The States of Jersey and the National Crime Agency. A Data processing agreement is in place for the Home Office and its sub processors DSA's are completed as part of any new law enforcement agency onboarding to the PND. The Home Office PND team are supported by a Data Protection Policy advisor who is engaged in reviewing all appropriate documents and agreements. The NPCC PND have support from NPCC Data Protection officer and other Police Data Protection and Information Assurance leads.
IR28. There is an absence of a data processing contract (where one is required)	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Implement and maintain necessary data processing contracts	Data Processing Contracts and Data Sharing Agreements are reviewed when appropriate. Data governance is a firm part of the PND governance and the need for DSA's and DPC's will be identified and resolved. The Lead Controller is responsible for data protection issues, including monitoring and approving data processing contracts. PND portfolio will support the recently adopted NPCC data governance for national data sets. Police Scotland adheres to the NPCC governance approach but currently has not appointed the NPCC as a legal agent to sign data processing contracts on its behalf.
IR29. Generally there is inadequate governance for the information	**1 Remote**	**2 Significant**	**1 Low**	**Treat**	Designate, train and task an information asset owner for the information	The NPPC PND lead is lead controller for the PND. They chair a quarterly National Steering Group, which reviews data and information risk as part of the schedule. The NPCC PND lead is supported by DP and IA leads from their host Force and the NPCC. The Home Office program has a law enforcement data protection policy advisor who is engaged and who supports program governance and work. The PND onboarding process focusses on information governance to ensure the right agreements are in place and the data protection tests are met. The NPCC PND lead, as joint controller, provides decision making regarding significant data quality issues and the onboarding of new agencies.

Ethical-related	Likelihood	Severity	Overall Risk	Decision	Potential Risk Treatment	Risk Treatment to be adopted/Comments
IR30. The information is inappropriately discriminatory	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Implement measures to ensure that the collection and use of the information does not inappropriately discriminate against certain groups, in particular children	Equality testing has been completed for the algorithm used for facial searching against data sets including ethnicity and gender. Further information is provided at risk IR32 As PND is a mirror of source systems, source system controllers are responsible for implementing measures to ensure the data collected into their source systems does not inappropriately discriminate. PND has an audit function which could identify trends or inappropriate use which may highlight information is being used inappropriately.
IR31. Data Subjects are unaware of their rights regarding the information	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Ensure that Privacy/Fair Processing Notices provide details of data subjects' rights and how to exercise them	See IR 15
IR 32. Unlawful and unfair processing of facial images (biometric data)	**2 Possible**	**2 Significant**	**2 Medium**	**Treat**	Effective training and Continuous Professional Development Clear direction within appropriate documents Equality testing of facial algorithms. Governance and review to identity bias based on race or gender. Reviewing Equality Impact Assessment Monitoring and review of operational facial search usage	Algorithm testing was undertaken by the Home Office in November 2021 to understand the comparative difference in performance between the face matching algorithm installed in 2016 and its 2021 replacement. The report found that the 2021 algorithm could find seven times more correct matches than its predecessor and generated 70% fewer incorrect matches for non-white faces. The PND Codes of Practice and Manual of Guidance directs a search using the PND must be for a policing purpose. College of Policing training and the Manaula of Guidance provides direction on how to use the facial search capability. Users of PND are trained and vetted, training and CPD focuses on the use of facial searching and enforces the need for searches to be for a policing purpose, that search results must be visibly assessed by trained officers and staff and must only be used as intelligence. The Facial search is retrospective using images which have been obtained for a lawful purpose. Images are gained from crime scenes and compared against lawfully held images. It is not a 'live' system obtaining facial images of members of the public. The National Steering Group, Home Office PND program and the NPCC PND lead are engaged in national facial recognition groups, assessing and reviewing performance and development of facial technology. Facial search statistics are provided in regular service reports, at Regional and National governance and are subject of review.

						PND has an audit function to protect against unlawful use of search functions. Audit is used to monitor the use of facial searching. PND uploads police images from police source systems, which have retention, review and delete regimes following the codes of practice of the Police Information and Records management and guidance provided by Authorised Professional Practice from the College of Policing. Appropriate Policy Document completed and will be reviewed when change is required or annually. **Update September 2024** Further testing was completed on the facial algorithm by the National Physical Laboratory, (NPL). The NPL tests found that facial search results were more likely to incorrectly display images of people with protected characteristics. In response to the test results, the following activity has been completed. College of Policing, CoP, have developed training products to re-enforce established training, guidance and practice, reminding PND users that facial search results are not evidential, they must be treated as intelligence, visibly assessed by PND users/investigators and other lines of enquiry considered before any positive action is taken. PND Manual of Guidance, MOG, provides directions to PND users on how to manage facial searching. This aligns with established and delivered CoP training. Additional manual safeguards have always been in place, even before NPL testing findings. These safeguards ensure the technology does not solely inform operational decisions.

						October 2024 NPCC PND lead directed an increase in the threshold of the facial algorithm. This significantly reduced the bias for the identified protected characteristics. The performance of the increase will be monitored and reviewed. CoP shared training material focused on facial search with PND users and Forces. Training material is available on PND Microsite and Knowledge Hub. **November 2024** Equality Impact Assessment completed based on the initial response to the NPL testing. Following operational feedback from Police Forces, which showed a significant detrimental impact on operational effectiveness and an increased risk to public, algorithm was reduced to original setting. Mitigation remains in place, use of established practice, visual checks and assessment before action, new training guides published and messaging completed. NPCC lead remains satisfied that the algorithm is not solely informing operational decisions. The additional manual safeguards ensure trained police officers and staff make the decisions on how to use the facial search results. The Home Office are exploring options to improve the facial matching technology used within the PND **April 2025** NPCC PND Lead has reviewed the decision to reduce the algorithm setting and was satisfied to maintain the algorithm setting. EIA has been updated and reviewed **July 2025** NPCC PND lead briefed Chief Constables Council on the NPL test results and gained support for the following actions, Requirement for an Equality Impact Assessment (EIA) to be conducted by each force to satisfy the Public Sector Equality Duty (PSED) obligations in respect of using RFR in PND. Ensure each Force has an internal documented policy and procedure that complies with the PND RFR training set out by the College of Policing and PND manual of guidance

					Forces to create a suitable governance regime to internally monitor and provide assurance of your compliance. Quarterly reporting to the PND National Steering Group on your compliance. **August 2025** Confirmation from all Police Forces and the NCA acknowledging the requirements within the letter and have appointed a lead to deliver the actions. **September 2025** Operational briefings provided by the NPCC PND portfolio for all Police Forces to ensure they are supported to comply with the directions in the July 2025 letter. **October 2025** NPCC PND Lead has reviewed the decision to reduce the algorithm setting and was satisfied to maintain the algorithm setting. EIA has been updated and reviewed. **November 2025** At the PND National Steering Group on 27th November 2025, chaired by the NPCC PND lead, Forces reported their compliance with the College of Policing training, PSED obligations and provided monitoring data. No Forces reported any adverse incidents, (a person being wrongfully arrested because of a PND facial search). EIA updated and reviewed
IR 33 New data feeds introduced to the PND	**1 Remote**	**2 Significant**	**2 – Low**	**Treat**	Accountable and clear data governance to include sharing agreements, processing contracts and DPIA's. Clear guidance and training for PND users Access Controls used effectively informed by the DSA.	New data feeds will be added to the PND as access to the PND is expanded to more Law Enforcement agencies. Law Enforcement agencies will only provide new data feeds if a lawful purpose exists, it is compliant with a DPIA and a DSA which have been approved by their Information Asset Owner and the NPCC PND lead. Establishing a new data feed is managed carefully using project governance and appropriate leads from the Home Office, NPCC and the Law Enforcement Agency.

					Effective management of the data feed to include testing, review and audit.	Governance and review are applied through the process to ensure data can be shared legally, there is a secure and effective and technical method to share the data.

.

Step 6: Assess Data Protection Compliance

The NPCC Data Protection Officer will complete this step with assistance from the Business SME, Business Lead and other associated Data Protection professionals, as is necessary.

Processing for Law Enforcement Purposes

Law Enforcement 1st Principle (Lawful & Fair)

(DPA Part 3 Section 35)

Requirement	Compliant?
LE1. No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA)	**Yes – no prohibitions identified, beyond those which may arise from the application of an individual's data subject rights.**
LE2. The processing is authorised by either statute, common law, royal prerogative or by or under any other rule of law	**Yes – collection and use of intelligence for police forces fits under Common Law policing powers/purposes and similar powers given to the NCA.**
LE3. Either of the following two processing conditions under DPA Part 3 Section 35(2) apply: Consent has been obtained, in compliance with ICO Guidance, or Processing is necessary for task carried out by a competent authority;	**Yes – the basis for processing will be necessity for the performance of tasks by the law enforcement organisations that act as Controllers for the PND.**
LE4. Where **Sensitive Processing** occurs either of the two following cases exist: DPA Part 3 Section 35(4) - Consent has been obtained, in compliance with ICO Guidance and an appropriate policy document exists as per DPA Part 3 Section 42. or DPA Part 3 Section 35(5) - Processing is strictly necessary, an Appropriate Policy Document exists as per DPA Part 3 Section 42, and one of the following DPA Schedule 8 conditions is met: 1 Statutory etc. purposes 2 Administration of justice 3 Protecting individual's vital interests 4 Safeguarding of children and of individuals at risk 5 Personal data already in the public domain	**The second case is used.** **NPCC and the Controllers have each produced Appropriate Policy Documents as part of their wider Data Protection compliance activities.** **The primary Schedule 8 ground is:** **1 - *Statutory etc purposes*** **1. The processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law (Common Law), and is necessary for reasons of substantial public interest.** **Grounds 2, 3, 4, 5, 6, and 9 are also likely to apply, in particular circumstances.**

6 Legal claims 7 Judicial acts 8 Preventing fraud 9 Archiving etc;	
LE5. The processing is in accordance with data subjects' reasonable expectations (fair); measures to provide privacy information are in place; Privacy Notices adequately describes the purpose and provide information about specific categories of processing including retention periods and transfers.	**Yes – data subjects will reasonably expect the police to collect, create and use their personal data. PND organisations' privacy notices should support that position.**

Law Enforcement 2nd Principle (Specific, Explicit & Legitimate Purpose)
(DPA Part 3 Section 36)

Requirement	Compliant?
LE6. The purpose for collecting the personal data is specified, explicit and legitimate	**Yes – Various Law Enforcement Purposes as described within this DPIA.**
LE7. Processing is compatible with the purpose it was collected for	**Yes – as above. If the personal data is subsequently used for a general purpose that will only occur where the law permits.**
LE8. Personal data collected for the law enforcement purpose is not otherwise processed unless it is authorised by law to do so	**Yes.**

Law Enforcement 3rd Principle (Adequate, Relevant & Not Excessive)
(DPA Part 3 Section 37)

Requirement	Compliant?
LE9. Adequate for the purpose	**Yes – PND organisations will follow national guidance and policy design to ensure intelligence is of the necessary standard for collection/creation, including its adequacy, relevance and data minimisation.**
LE10. Relevant to the purpose	
LE11. Not Excessive for purpose	

Law Enforcement 4th Principle (Accurate & Kept-up-to-date where necessary)
(DPA Part 3 Section 38)

Requirement	Compliant?

LE12. Is accurate with distinction between fact-based and opinion-based	**Yes – processes are in place to ensure accurate recording and any necessary distinction between opinion is apparent.**
LE13. Is kept up-to-date where necessary	**Yes –at a record level records will be updated as is necessary, but some records will not be subject to updating due to their evidential nature.** **At a dataset level records will be deleted from the PND when the originating Controller removes it from their source systems.**
LE14. Distinguishes between suspects, offenders, victims, witness & others where relevant	**Yes – business processes, national guidance and local policy ensure these distinctions are apparent.**
LE15. Is erased or rectified if inaccurate without delay	**Yes – PND organisations have processes in place to ensure rectification occurs where required.**
LE16. Is not transmitted or made available if inaccurate, incomplete or out-of-date	**Yes – PND organisations have in place measures to ensure substandard data is not disseminated/made available.**

Law Enforcement 5th Principle (Kept no longer than is necessary)

(DPA Part 3 Section 39)

Requirement	Compliant?
LE17. Personal data is not kept longer than is necessary	**Yes – PND reflects the retention or deletion processes applicable to source data collections, which will be in accordance with the College of Policing APP or equivalent, and/or local policy in the case direct entry data.**
LE18. It is possible to justify the retention in relation to the purpose of the processing	**Yes – provided any deviation from agreed national policy also ensures this occurs.**
LE19. A written retention, review and deletion policy exists for the personal data	**Yes – College of Policing APP and NCA equivalent.**
LE20. Personal data is subject to periodic review and is anonymized, erased or disposed of when no longer needed	**Yes – as per the measures described above.**

Law Enforcement 6th Principle (Processed Securely)

(DPA Part 3 Section 40)

Requirement	Compliant?

LE21. Appropriate measures are in place or planned to prevent the personal data being accidentally or deliberately compromised	**Yes – multiple technical and organisational measures to ensure the confidentiality, integrity, and availability of PND data are employed by all PND organisations and the processors and sub-processors working on their behalf.**
LE22. Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach	**Yes.**
LE23. Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing	**Yes – training and vetting measures are adopted.**
LE24. Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) (DPA Part 3 Sections 67 and 68) involving the personal data	**Yes – the PND organisations have in place security incident management processes and the ability to escalate certain incidents to 'critical incident' status with central oversight by the PND Lead.**
LE25. DPA Part 3 Section 66 Security of processing requirements are met	**Yes – a complex range of measures are in place centrally and within the organsiations that use PND.**

Law Enforcement Accountability Requirement
(DPA Part 3 Section 34)

Requirement	Compliant?
LE26. It is possible to demonstrate compliance with all the Law Enforcement Principles	**Yes – this achieved by the JCA, DPIA, and other central and local documents.**

Other DPA Part 3 Controller & Processor Obligations
(DPA Part 3 Section 40)

Requirement	Compliant?
LE27. Compliance with Controller's general duties (DPA Part 3 Section 44)	**Yes – this is achieved via the Privacy Notices of the PND organisations.**

LE28. Appropriate technical & organisational measures, including policy as required by DPA Part 3 Section 56 are implemented;	**Yes – these are delivered by the range of measures to protect the confidentiality, integrity and availability of the PND data outline above.**
LE29. Data Protection by Design & Default requirements set out in DPA Part 3 Section 57 are met	**Yes – future developments to the PND will trigger the review and updating of this DPIA as the vehicle to ensure Data Protection by Design and Default.**
LE30. Where joint controllership exists that each parties' respective obligations under DPA Part 3 Section 58 to comply with the UK GDPR are documented	**Yes – a Joint Controllership Agreement has been developed for sign-off by the Controllers.**
LE31. Where a processor is employed DPA Part 3 Section 59 and 60 obligations are met including the requirement for a data processing contract to be place	**Yes – Contracts are in place with the Home Office as processor and between them and any sub-processor used.**
LE32. Records of processing activities are maintained in accordance with DPA Part 3 Section 61;	**Yes – each PND organisation should maintain their own RoPA on which Intelligence/PND processing is recorded.**
LE33. Logs are maintained in accordance with DPA Part 3 Section 62;	**Yes – in August 2023 the Home Office confirmed that the PND satisfies these requirements.**
LE34. Data Protection Impact Assessments (DPIA's) are conducted in accordance DPA Part 3 Section 64 and 65 where required	**Yes – evidenced by this DPIA and another for the Historic Data Wash which uses PND data.**

Law Enforcement International Transfers

(DPA Part 3 Section 37)

Requirement	Compliant?
LE35. Where the transfer is to competent authorities it is in compliance with DPA Part 3 Section 73 General principles for transfers of personal data, including where a third country is 'adequate' (DPA Part 3 Section 74) or where there are appropriate safeguards (DPA Part 3 Section 75), or special circumstances apply (DPA Part 3 Section 76). or Where the transfer is other than to competent authorities it is compliance with DPA Part 3 Section 77;	**Yes – this is relevant to transfers to the States of Jersey Police. No other international transfers occur.** **Recommendation – documentation is drawn up to show how international transfers to States of Jersey Police are compliant.**
LE36. Conditions regarding subsequent transfers are set as required by DPA Part 3 Section 78.	

LE37. Where the transfer is to competent authorities it is in compliance with DPA Part 3 Section 73 General principles for transfers of personal data, including where a third country is 'adequate' (DPA Part 3 Section 74) or where there are appropriate safeguards (DPA Part 3 Section 75), or special circumstances apply (DPA Part 3 Section 76). or Where the transfer is other than to competent authorities it is compliance with DPA Part 3 Section 77;	

Processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes
(DPA Part 3 Section 41)

Requirement	Compliant?
LE38. Where this applies this is compliant with DPA Part 3 Section 41.	**Not applicable.**

Processing for General Purposes

UK GDPR 1st Principle (Lawful, Fair & Transparent)
UK GDPR Article 5(a)

Requirement	Compliant?
G1. No rule of law prohibiting the processing is transgressed (including that arising from the application of any rights of rectification, erasure or restriction under the DPA/UK GDPR)	**Yes – no prohibitions identified, beyond those which may arise from the application of an individual's data subject rights.**
G2. One of the five available UK GDPR Article 6(1) **Processing Conditions** exists for all of the personal data including Special Category Data and Criminal Offence Data *(Note: The Police are unable to use (f) Legitimate Interests)*: (a) Consent; (b) Contract; (c) Legal Obligation; (d) Vital Interests;	**Yes – (c) processing is necessary for compliance with a legal obligation to which the controller is subject;*** **(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.** ***e,g, obligations arising from Police Act 1996 as amended**

(e) Public Task (see DPA Part 2 Section 8 for examples)	
G3. If **Consent** is used it complies with definition at UK GDPR Article 4(11), requirements at UK GDPR Article 7 (Conditions for Consent), and ICO Guidance (subject to exemption for **Special Purposes** at DPA Schedule 2 Part 5 Paragraph 24);	**Not applicable.**
G4. For any **Special Category Data** being processed, in addition to a UK GDPR Article 6(1) **Processing Condition** being met, one of the following UK GDPR Article 9(2) **Special Processing Conditions** applies: (a) Explicit Consent; (b) Employment, Social Security & Social Protection; (c) Vital Interests; (d) Political, Philosophical, Religious or Trade Union (e) Made Public by Data Subject; (f) Defence of Legal Claims; (g) Substantial Public Interest; (h) Health and Social Care; (i) Public Health; (j) Archiving, Research & Statistics **And** in the case of (b) Employment, Social Security and Protection, or (h) Health and Social Care, or (i) Public Health, or (j) Archiving, Research and Statistics, a condition in DPA Schedule 1 Part 1 applies; or in the case of (g) Substantial Public Interest, a condition in DPA Schedule 1 Part 2 applies And An **Appropriate Policy Document** is created and maintained in	**Yes – the most likely to apply are (c) vital interests, (f) defence of legal claims, and (g) substantial public interest.** **The relevant DPA Schedule 1 Part 2 conditions are:** **PND Organisations should already have in place Appropriate Policy Documents.**

accordance with DPA Schedule 1 Part 4 if a condition in DPA Schedule 1 Part 1 or 2 is used	
G5. If the purpose of the processing differs from the initial purpose when the data was collected, and the processing is not based on consent or law, compatibility of the new use is tested using UK GDPR Article 6(4)	**Yes – in most cases the processing will be reliant on a legal basis that permits the data to be passed from DPA Part 3 to UK GDPR. In other cases compliance with Article 6(4) should not be problematic.**
G6. For any **Criminal Offence Data** being processed, in addition to a UK GDPR Article 6(1) **Processing Condition** being met; compliance with UK GDPR Article 10 is achieved; a DPA Schedule 1 Part 1, 2 or 3 is condition is met, an **Appropriate Policy Document** is created in accordance with DPA Schedule 1 Part 4; and the processing is authorised by law as a clear and foreseeable application of a common law task, function or power, a statutory provision, or statutory guidance	**Yes – processing is carried out only under the control of official authority or when the processing is authorised by law providing appropriate safeguards for the rights and freedoms of data subjects. The DPA Schedule 1 conditions most likely to apply are 4 research, 6 necessary for exercise of a function confirmed by a rule of law and is in the substantial public interest, 7 for the administration of justice, 8 equality of treatment, 10 preventing and detecting unlawful acts, 11 protecting the public against dishonesty, 13 journalism (special purposes), 18 safeguarding of children and of individuals at risk, 30 protecting individuals' vital interests, 32 personal data in the public domain, 33 legal proceedings PND organisations will have in place APDs.**
G7. Fairness & Transparency requirements under UK GDPR Articles 12 13 14 are met	**Yes – through PND organisations' privacy notices.**
G9. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified.	**Yes – these are used where appropriate, proportionate and necessary.**

UK GDPR 2nd Principle (Purpose Limitation)

UK GDPR Article 5(b)

Requirement	Compliant?
G10. Processing is in a manner that is compatible or where is for archiving in public interest, scientific or historical research or statistical purposes is exempt from that requirement by virtue of UK GDPR Article 89(1)	**Yes – for various purposes outlined in this DPIA.**
G11. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2	**Yes – these are used where appropriate, proportionate and necessary.**

Disclosure Required by Law. DPA Schedule 2 Part 1 Paragraph 3 **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26	

UK GDPR 3rd Principle (Data Minimisation)

UK GDPR Article 5(c)

Requirement	Compliant?
G12. Personal data is adequate for the purpose(s) of processing	**Yes – PND organisations will follow national guidance and policy design to ensure intelligence is of the necessary standard for collection/creation, including its adequacy, relevance and data minimisation, and where any personal data involved is subsequently used for General Purposes compliance is achieved against relevant organisational and national guidance and policies.**
G13. Personal data is relevant for the purpose(s) of processing	
G14. Personal data is limited to that required for the purpose(s) of processing	
G15. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Crime & Taxation.** DPA Schedule 2 Part 1 Paragraph 2 **Disclosure Required by Law.** DPA Schedule 2 Part 1 Paragraph 3 **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26.	**Yes – these are used where appropriate, proportionate and necessary.**

UK GDPR 4th Principle (Accuracy)

UK GDPR Article 5(d)

Requirement	Compliant?
G16. Personal data is accurate for the purpose(s) of the processing	**Yes – processes are in place to ensure accurate recording and transcription of any personal data.**
G17. Personal data is up-to-date where necessary for the purpose(s) of the processing	**Yes – processes are in place to update records where necessary.**
G18. Personal data is erased or rectified without delay where required	**Yes – processes are in place to ensure personal data is rectified where necessary to do so.**

G19. Consideration is given to the appropriate use DPA Schedule 2 exemptions where justified including: **Special Purposes.** DPA Schedule 2 Part 5 Paragraph 26.	**Yes – these are used where appropriate, proportionate and necessary.**

UK GDPR 5th Principle (Storage Limitation)

UK GDPR Article 5(e)

Requirement	Compliant?
G20. Personal data enabling the identification of data subjects is retained no longer than is necessary for the purpose(s) of the processing,except where continued retention is solely for archiving in the public interest, scientific or historical research or statistical purposes in accordance with UK GDPR Article 89 & measures required by the UK GDPR are in place to safeguard the rights and freedoms of the data subjects.	**Yes – PND reflects the retention or deletion processes applicable to source data collections, which will be in accordance with the College of Policing APP or equivalent, and/or local policy in the case direct entry data.**

UK GDPR 6th Principle (Integrity & Confidentiality)

UK GDPR Article 5(f)

Requirement	Compliant?
G21. Appropriate measures are in place to prevent the personal data being accidentally or deliberately compromised	**Yes – multiple technical and organisational measures to ensure the confidentiality, integrity, and availability of PND data are employed by all PND organisations and the processors and sub-processors working on their behalf.**
G22. Those measures are commensurate to the nature of the personal data and the nature of harm that could result from a compromise or data breach	**Yes.**
G23. Those measures include physical, technical, and procedural types and have been developed in consideration of the reliability and training of staff involved in the processing	**Yes.**
G24. Appropriate measures are in place to swiftly and effectively identify, respond to and manage information security incidents and data breaches (including notification to the Commissioner and data subject) (UK GDPR Article 33 and 34) involving the personal data	**Yes.**
G25. UK GDPR Article 32 Security of processing requirements are met	**Yes.**

UK GDPR Accountability Requirement

UK GDPR Article 5

Requirement	Compliant?
G26. It is possible to demonstrate compliance with all the UK GDPR Principles	**Yes – this achieved by the JCA, DPIA, and other central and local documents.**

Other UK GDPR Controller & Processor Obligations

Requirement	Compliant?
G27. Appropriate technical & organisational measures, including policy as required by UK GDPR Article 24 are implemented	**Yes.**
G28. Data Protection by Design & Default requirements set out in UK GDPR Article 25 are met	**Yes – future developments to the PND will trigger the review and updating of this DPIA as the vehicle to ensure Data Protection by Design and Default.**
G29. Where joint controllership exists that each parties' respective obligations under UK GDPR Article 26 to comply with the UK GDPR are documented	**Yes – a Joint Controllership Agreement has been developed for sign-off by the Controllers.**
G30. Where a processor is employed UK GDPR Articles 28 and 29 obligations are met including the requirement for a data processing contract to be place	**Yes – Contracts are in place with the Home Office as processor and between them and any sub-processor used.**
G31. Records of processing activities are maintained in accordance with UK GDPR Article 30	**Yes – each PND organisation should maintain their own RoPA on which Intelligence/PND processing is recorded.**
G32. Data Protection Impact Assessments (DPIA's) are conducted in accordance with UK GDPR Articles 35 and 36j where required	**Yes – evidenced by this DPIA and another for the Historic Data Wash which uses PND data.**

Where necessary, consider restricted transfers of personal data for general processing purposes to countries or territories beyond the European Union or to international organisations (**third countries)**

Requirement	Compliant?
G33. The restricted transfer is in compliance with UK GDPR Article 44 General principles for transfers of personal data, including where a third country is 'adequate' (UK GDPR Article 45) or where there are appropriate safeguards (UK	**Yes – this is relevant to transfers to the States of Jersey Police. No other international transfers occur.**

GDPR Article 46, 47 or 48), or an GDPR Article 49 condition applies.	**Recommendation – documentation is drawn up to show how international transfers to States of Jersey Police are compliant.**

Step 7: Sign-off and record of outcomes

Consultation Outcomes

Summary of consultation responses (if conducted):

Not applicable.

Summary completed by:

Not applicable.

Date completed:

Not applicable.

Business Lead's response to consultation responses (if conducted)

Not applicable.

Date completed:

Not applicable.

Data Protection Officer Comments

Data Protection Officer's comments, including whether the DPIA has been conducted appropriately and whether it must be sent to the ICO for review:

I confirm that in my opinion this DPIA is comprehensive, thorough, and identifies and considers all relevant privacy risks. It is my assessment that the processing of personal data on the PND is not of a nature that the risks to the rights and freedoms of individuals are so high that it hits the threshold for reporting to the ICO.

I recommend that this document is shared with the NPCC Data Sharing Quality Assurance Panel for review and comment, amended as necessary, and then passed to the NPCC PNC Lead to consider the DPIA and complete the section below.

I also recommend that the DPIA remains a 'living document' and is reviewed and updated where necessary should there be any significant changes in the use of PND data, the technology it is housed within, or should there be a critical cyber or data breach. I will review any future iterations of this DPIA.

NPCC DPO

Date completed:

15th August 2023.

Business Lead's Comments

Business Lead's confirmation of agreement with risk assessment, acceptance of identified responses to risks, consideration of Data Protection Officer's comments and acceptance of responsibility to update this DPIA as is necessary.

I agree with risk assessment, accept the risks and accept responsibility to update the DPIA as necessary

NPCC PND Lead

Date completed:

28th November 2025