Home Office

National Law Enforcement Data Programme

Law Enforcement Data Service (LEDS) – Privacy Impact Assessment Report

Published: July 2018

Contents

1. Executive Summary

This document sets out the results of a Privacy Impact Assessment (PIA) looking at the development of the Law Enforcement Data Service (LEDS) by the National Law Enforcement Data Programme (NLEDP).

The Programme will support Law Enforcement and other competent authorities with current and joined-up information, on-demand and at the point of need, in order to prevent crime and better safeguard the public. It will replace the existing Police National Database (PND) and the Police National Computer (PNC) with the new LEDS. The new platform will potentially allow addition of new data sets at a later date.

PNC was first used in 1974 and continues to run on broadly the same technology as it did at that time. PNC allows the sharing of records of interactions with the police, law enforcement agencies and the criminal justice system. PND is more modern, having been introduced as a recommendation following the Bichard enquiry into the Soham Murders. The Bichard report recommended a national system for sharing police intelligence to ensure better protection for the public.

This Privacy Impact Assessment (PIA) relates to data processing undertaken in the PND and PNC and provides a current view of the expected privacy impacts for LEDS. This PIA replaces the existing PND PIA and constitutes the first such impact assessment for the PNC; and considers processing within these systems prior to 25 May 2018 and the entry into force of the Data Protection Act 2018 (DPA). Final sign off was obtained on 02 May 2018.

This publication is the first version of what is intended to be an annual series of LEDS privacy assessments; future versions will focus on LEDS as the new service and use the new Data Protection Impact Assessment (DPIA) process according to the DPA.

The Programme conducted this PIA at the request and on behalf of PNC, PND and future LEDS Data Controllers in the Home Office's capacity as the provider of the Service. This document therefore complements and must be read in conjunction with any operational impact assessments produced by the user organisations.

The following primary risks and subsequent mitigations are identified within this document, organised by associated system:

Issue	Concern	Mitigation
PND		
Facial search	Inconsistent application of common retention policy for custody images at a local force level.	Local custody image retention policy is under review to ensure retention length is necessary and proportionate.
Data quality	Data held on local force systems that feed into PND varies in quality and structure and accuracy. Inconsistency in local force data quality impacts on PND data quality.	Subject to resourcing, compliance with existing policing guidance on the management of police information (MoPI) may be thoroughly addressed. A Programme-led project dedicated to Data Standards is working with PND Users to improve PND data quality standards.
PNC		
Proportionality of holding certain records	The retention of arrest data (not charged or convicted), charging data (not convicted) or very minor historical conviction data can be	The proportionality of holding this data is under review, including primarily

	perceived as not proportionate in data protection terms.	considerations regarding the purpose for which this data is held on systems.
LEDS		
Potential consequences of co-location / merging of data	Greater amounts of data are made available to Users – in both volume and type – that hinder rather than benefit Users' strategic or tactical objectives due to information overload.	Considered mitigations include partitioning specified data pools, rather than fully merging them, on LEDS. Detailed access-based-controls for both roles and organisations are also being developed within the Programme and will be clearly marked within Data Sharing Agreements.
	Some Users are able to access a greater-than-appropriate level of data for their individual role or organisation.	
	Individuals are brought to the attention of Law Enforcement Agencies for the wrong reasons or through inappropriate means.	
	Quality of PNC data is adversely affected by corresponding PND data.	
	Conflicts arise as a result of differing data management strategies in different User organisations.	
Retention variance	Retention periods vary between PND and PNC.	Whether or not to maintain data separation with specific retention regimes for data based on its provenance or to move to a single retention regime, likely based on MoPI, remains under consideration.

This document should be read in conjunction with the PND Code of Practice, PND Manual of Guidance, the PNC Code of Practice, the PNC Manual of Guidance and the ACPO/ACPOS Information Systems Community Security Policy for the express purpose of policing.

Policing purpose is wider than the Police Service and includes United Kingdom Law Enforcement agencies who can demonstrate a Policing Purpose as defined in the ACPO MOPI (Management of Police Information) guidance and Code of Practice. References to ACPO guidance (the Association of Chief Police Officers) should be taken to refer to guidance issued from time to time by the National Police Chief's Council (NPCC) which succeeded ACPO on April 01st 2015.

2. The National Law Enforcement Data Programme

Background

Law enforcement agencies in the United Kingdom currently utilise a wide variety of information systems at a local level to collect and process data in connection with their policing purpose. It has also been recognised that there is great value in being able to share relevant information across law enforcement agencies in a timely and effective fashion. There are a number of national systems which enable them to do this, the most significant being:-

- the Police National Computer (PNC), introduced in 1974, which holds personal data and other information relating to individuals (nominals) including arrests, charges & court disposals (including convictions), together with other information about vehicles and property; and
- the Police National Database, introduced in 2009, which receives intelligence data from law enforcement agencies (predominantly police forces) on a daily basis concerning persons, events, locations, organisations (including criminal) and objects, and is accessible by authorised users from those organisations.

Both systems have been in use for some years and the technology used is becoming more difficult and expensive to support and maintain, providing a strong incentive to upgrade both systems in line with modern requirements.

The National Law Enforcement Data Programme

The National Law Enforcement Data Programme (NLEDP) aims to relocate the currently separate PNC and PND systems onto a single technology platform: the Law Enforcement Data Service (LEDS). The intention is to support Law Enforcement and other agencies with current and joined up information, on-demand and at the point of need, in order to prevent crime and better safeguard the public.

The key objectives of the programme are to deliver a

Law Enforcement Data Service (LEDS) that will:

- rationalise national information systems;
- enhance the national information data set;
- deliver more service capabilities from the national information data set; and
- reduce the cost of providing and maintaining national information.

The data sets from both PND and PNC will co-locate onto LEDS to improve accessibility for those users that need access to the suite of data sets for matching, where possible, whilst security provision will be effected to retain separation for those users that need access only to specific data sets. This interoperability will provide law enforcement agencies with an enhanced set of national information accessible through a single route for the first time.

Benefits will include faster and improved searching of records, better identification of individuals and more effective information sharing between law enforcement and other authorised organisations. The expectation is that PND data will be moved onto the LEDS platform during 2018, followed by the PNC data during 2019.

The NLEDP is part of a larger programme of work including the Home Office Biometrics Programme (HOB) and the Emergency Services Mobile Communications Programme intended to develop and provide improved technology resources for UK law enforcement agencies.

3. Privacy Impact Assessments and why the Programme decided to conduct one

3.1 The issue of the Privacy Impact Assessment (PIA) handbook by the Office of the Information Commissioner in 2007 recommended PIAs as good practice for any initiative involving new or significant changes to the processing of personal information. This was followed in February 2014 by the Conducting Privacy Impact Assessments Code of Practice published by the Information Commissioner's Office with updated guidance on how to conduct a PIA.

3.2 The Information Commissioner suggests, in the Code of Practice, the type of project which might require a PIA including:

- *'A new IT system for storing and accessing data."*
- *"A data sharing initiative where two or more organisations seek to pool or link sets of personal data.*
- *"Using existing data for a new or unexpected or more intrusive purpose"; and*
- *"A new database which consolidates information held by separate parts of an organisation".*

3.3 The LEDS platform can be seen as a new IT system for storing and accessing data; as data currently held on two separate systems, PNC and PND, will be moved from these locations to sit on the LEDS platform, designed specifically for this purpose. It will allow authorised users to access data from both sources, potentially via a single search. This might result in existing data being used for a more in depth purpose because the co-location of data from both systems (and from others which may be relocated to the platform in the future) may return a larger number of results, including personal data, which otherwise might not have been offered about individuals previously, particularly where no wrongdoing is suspected. In the longer term, the Programme seeks to enable further data sharing between a range of organisations in the law enforcement field, by the addition of more systems to the platform or through links to systems owned by other organisations, such as Border Force, to enable a more "joined up" approach in the law enforcement field. This arguably has the potential to impact adversely on the privacy of individuals and may also raise some concerns with those who question access to, and use of, their personal data by Government organisations for purposes which may not be clear to them.

3.4 In terms of LEDS, the purposes of carrying out a PIA were to:

- Identify and manage the risks that privacy issues represent to realising the intended benefits of LEDS.
- Generate information to aid decision making and support good governance and business practice around information processing.
- Identify any necessary privacy features so these can be designed in rather than be subject to costly retro-fitting at a later stage.
- Allow privacy considerations to be built into the design from the outset to provide a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer service life.
- Promote public confidence to maximise the support from the public for information collection by the police and reduce the risks of privacy-related incidents that could undermine public confidence in the Police Service, or the Government.

3.5 The PIA process is also an opportunity to consider the privacy risks in relation to PND and PNC. A full scale Privacy Impact Assessment, based on the Privacy Impact Assessment (PIA) handbook, was carried out during the project stage of PND and published in 2009; it was subsequently reviewed in 2013. Since that time a number of additional facilities such as facial search have become available and the privacy implications of these require consideration. PNC

was introduced into service in 1974, prior to the passing of any data protection legislation. Even when PIAs were introduced the requirement was only for new projects or activities: PNC was an existing system so no PIA was carried out.

3.6 This PIA initial review is being conducted for the purposes of informing the development of the LEDS platform, including the relocation of the PND and PNC systems onto this platform and management of the associated issues which may arise.

3.7 Further PIA updates will be conducted as the Programme progresses to capture and address privacy issues that may develop or become apparent as well as to record the decisions made in relation to issues identified during the conduct of this initial PIA iteration. As a minimum, the PIA will be updated or refreshed on an annual basis.

4. Methodology

4.1 The handbook published by the Information Commissioner advocates an initial screening to decide whether a PIA is necessary. The initial screening involves considering a number of questions that are set out in the handbook.

4.2 The Programme conducted an initial screening assessment in November 2016, looking ~~at~~ PNC and PND as separate entities (as they currently exist) whilst also considering the potential privacy issues that might arise from co-location of both systems on the LEDS platform. The screening questions, and the Programme's answers to them, are included at Annexes A & B. These were discussed with members of the Programme and also with the Information Commissioner's Office. The results of the initial screening pointed to the need to conduct a PIA.

4.3 The PIA Code of Practice suggests the following form and structure for a PIA:

- Describing the information flows – looking at what information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information.
- Identifying the privacy and related risks – this includes risks to individuals such as damage caused by inaccurate data or a security breach; it also includes distress from an unnecessary intrusion into an individual's privacy. Risks to the organisation should also be considered such as loss of reputation or the financial consequences of a data breach. Consideration must also be given to legal compliance risks.
- Identifying and evaluating privacy solutions – consideration of how each privacy risk can be eliminated or reduced to an acceptable level, including evaluating the likely costs and benefits of possible options.
- If relevant, conduct:
    - Privacy law compliance check - focuses on compliance with various "privacy" laws such as Human Rights Act, Regulation of Investigatory Powers Act and Privacy and Electronic Communications Regulations as well as the Data Protection Act. Examines compliance with statutory powers, duties and prohibitions in relation to use and disclosure of personal information. See Annex C.
    - Data protection compliance check – a checklist for compliance with DPA. Usually completed when the project is more fully formed.
- Recording the PIA outcomes – A PIA report should summarise the process and the steps taken to reduce the risks to privacy, recording the decisions taken to eliminate, mitigate or accept the identified risks. These decisions should be signed off at an appropriate level.
- Review – This sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. It looks at new aspects of the project and assesses whether they should be subject to a PIA.

4.4 For the initial iteration of the PIA, it was decided that consultation would be limited to a small number of interested parties, listed in Annex D; however, the expectation is that, in view of some of the issues identified during the initial PIA process and their significance in relation to the design and development of the LEDS platform, a broader consultation with stakeholders will take place during the course of developing further iterations of this PIA.

4.5 In addition to the consultation, extensive internal analysis has been carried out, looking at relevant issues in relation to the PND and PNC systems, together with additional issues arising from their co-location on a single platform. A number of significant issues have been

identified which will be further explored as part of the project and the outcomes used to inform the development of the platform, particularly in relation to measures to protect and enhance privacy.

4.6 In carrying out this work, it was the Programme's aim not just to make sure that it was meeting the minimum legal requirements but to minimise, as far as possible. given the Programme's aims of supporting law enforcement and protecting the public, the impact on individuals' privacy – i.e. to be "privacy-friendly", not just "privacy-compliant". The Programme is following the concept of "privacy by design", incorporating privacy and security measures at the design stage of the project in line with current good practice.

4.7 The detailed requirements that involve IT will be fed into the business requirements supplied to the project architects, and subsequently the appointed supplier, to address the design, build and operation of the system. Those that involve business process redesign will inform work to set policies and business rules for the data to be located on the LEDS platform and the future use of the system.

4.8 As this work progresses, account will be taken of new legislation, reports, reviews and recommendations as they become available. At present, these include:

- PND: Code of Practice on the Operation and use of the Police National Database (March 2010)
- Information Systems Community Security Policy: Strategy for the Police Community (March 2009)
- Police Information: Guidance on the Management of Police Information (April 2010)
- National Information Risk Appetite Statement (December 2011)

4.9 The initial internal analysis and intended relocation of the PND and PNC systems were discussed with the Information Commissioner's Office and their views obtained; ongoing liaison with the ICO will inform the future development of the system in relation to privacy issues.

4.10 Section 8 sets out the plans for formally reviewing, auditing and updating this assessment. However, work will continue to ensure that privacy requirements are fully considered in the detailed design of the LEDS and the business processes around the data located on it.

5. The Police National Database, its associated processes and privacy concerns

5.1 The PND holds detailed information on people (e.g. names), objects (e.g. cars), organisations (e.g. companies), organised criminal gangs, locations (e.g. addresses) and events (e.g. crime reports). Chief Officers are owners (and data controllers) for the information loaded onto the PND or created on the system by their staff. This means that Chief Officers will continue to be responsible for the data, including any links made with other information. Data supplied by other UK law enforcement agencies will be the responsibility of their Chief Officers or similar grade.

5.2 PND's capabilities **can** be described as follows: -

- Data Upload and Entry allows forces to share copies of information (including images, files, maps, video and audio) held on their local systems with each other and also to enter information onto the PND directly. Users are able to create links between records, including where the records belong to different forces.
- Search and Retrieve allows users to find and view information on PND using both simple free text searches and more sophisticated searches which allow the scheduling of searches to run at certain times, triggered when certain keywords/criteria are met, association searches and alerts via SMS/email for searches; it also helps to identify links with other information. Mapping functionality for location data on UK maps is also provided, together with flagging functionality to highlight certain information. It is also possible to transfer data from PND to other systems used by forces to carry out more sophisticated analyses.
- The PND Facial Search facility, added in 2014, enables authorised users to upload an image from an external source such as a still image from CCTV footage into the PND and search across all person images attached to person records or custody records (England and Wales) to see if there are any suggested matched images; there are currently about 12 million images enrolled into the PND gallery. The image being uploaded is known as the probe image and PND compares that image against all other images held in the system. This takes place in an area of the system known as the gallery. Probe images are not retained on the PND system after a search has been conducted except for audit purposes. The matching of images is not entirely automated; the user's human eye will be the deciding factor in concluding that two separate photographic images relate to the same subject. The match results are not used for evidential purposes but are treated as intelligence.
- Security and Audit help to ensure that the information is kept safe. Only authorised users are permitted to access the system and they can only view the information that they need for their role within the organisation they work for; for example, access to information about child protection is restricted to those police staff involved in child protection work. All user activity on the PND is auditable; the details of all transactions on the system and the results generated by those actions are logged and subject to audit by force or other designated auditors.
- Communication capabilities are used for purposes ranging from very urgent messages (e.g. a terrorist threat) to routine data quality issues (e.g. signalling potential duplicate or incorrect records). "Flags" and "Markers" can also be added to records, which allow users to provide additional information about, or register an interest in, a record.

- The Review, Retention and Disposal (RRD) function, in line with MoPI, allows forces to re-examine the information they hold to decide whether they need to retain it and, if not, to dispose of it whilst an alerts functionality within PND indicates when data requires review/disposal. RRD can be complex because a decision by one force to dispose of one of its records might affect another force which still needs the information it contains. Decisions about whether to dispose of information may also be affected by information held by another force.
- System Administration – As PND is rule-driven, this function allows these rules to be set and amended as necessary. It also allows administrators within each force to manage their authorised users and their access to data.

5.3 A number of features of the PND itself help to make it privacy friendly. These include:

- safeguards to ensure that the system is only accessible by authorised, trained users;
- users are only able to access the type of information and facilities that they need to do their job;
- all use of the system is logged and subject to audit;
- the original PND capabilities were designed with full consideration of privacy requirements;
- rules for the use of the system, and of any information obtained from it, are set. These include that the system and data must only be used for policing purposes[1].

Safeguarding access to the system and its data

5.4 PND is capable of holding information classified up to CONFIDENTIAL according to the Government Protective Marking Scheme (GPMS)[2] and the entire system was classified as CONFIDENTIAL up to 2014 with commensurate security measures put in place to secure data at this level. However, it was recognised that, in view of the fact that less than 1% of the data held on PND is actually CONFIDENTIAL, classifying the entire system at this level was excessive and a hindrance to police forces in achieving best results from the ability to access intelligence information on a national basis in line with the recommendations of the Bichard report.[3] It was therefore agreed with the national accreditors that the majority of the system would be reclassified as RESTRICTED with the operative security measures within police forces adjusted to meet the new classification, thus allowing a larger pool of authorised users to access the RESTRICTED data; CONFIDENTIAL data continues to be subject to the higher security measures and access is limited to a small number of specialist users, ensuring its continued protection. GPMS has now been replaced across the public sector outside policing by the Government Security Classification Scheme[4]. It is expected

---

[1] Defined in the MoPI Code of Practice as: “protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; and any duty or responsibility of the police arising from common or statute law”.

[2] The GPMS was a system for protecting information, now largely replaced by the Government Security Classification Scheme in the public sector beyond the police service. It had 5 main levels of protective marking; In order of the increasing amount of harm that could be caused by unauthorised disclosure, these were: PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP-SECRET.

[3] Sir Michael Bichard, *‘The Bichard Inquiry Report’,* Home Office, 22 June 2004, <http://dera.ioe.ac.uk/6394/1/report.pdf>

[4] The Government Security Classification Scheme, introduced in April 2014, has replaced GPMS as the current system for protecting information. There are three classification levels, OFFICIAL, SECRET and TOP SECRET. These do not map directly across the classifications used under GPMS but, in general terms, data previously classified as RESTRICTED and some CONFIDENTIAL data would now be regarded as OFFICIAL with appropriate handling instructions being attached.

that the new LEDS platform will be classified as OFFICIAL, possibly with the handling instruction of OFFICIAL-SENSITIVE, but existing markings on data within the PND system will be maintained, as will the differential security measures accorded to the current data categories.

4.5 The PND is currently available to policing organisations over the Public Sector Network for Policing (PSNP). This enables direct access for the 43 forces in England and Wales, Police Scotland, British Transport Police, Police Service of Northern Ireland, the Service Police Crime Bureau and the National Crime Agency. A limited number of officers in the Disclosure and Barring Service, Border Force, Immigration Enforcement, Identity & Passport Services, HMRC and the Security Industry Authority (SIA) also have access. The Medicines and Healthcare Products Regulatory Authority (MHRA) are in the process of on-boarding to PND at present. These organisations provide relevant intelligence information to PND and are granted access to the information on the system supplied by other user organisations. 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.

4.6 The Identity and Access Management (IAM) system, working as part of PND, ensures that only authorised users can access the system. It uses a single digital identity utilising smartcard technology, meaning that it is not necessary to rely on less secure user passwords that can be compromised or shared, and that users are identifiable when they access the system directly. IAM also helps to ensure that any use of the PND can be traced through a rigorous and secure auditing process. IAM supports “Role Based Access Controls” which ensures that users only have access to capabilities and information that they need for their business role.

4.7 Controls determine which PND functions a user account can access, including the ability to control access to ‘Advanced’ functions such as more advanced searches (Association Searching, Start to End searching, Interest Search, Triggered Search and Scheduled Searches), Markers and Associations entry, Local Audit and Local Administration.

4.8 Due to the initial CONFIDENTIAL categorisation of the system, accessing of PND data via mobile data devices was not permitted as the security measures available were insufficient to protect data of this sensitivity. Reclassification of the data to RESTRICTED may enable PND data to be made available via mobile devices in the future.

Auditing use of the system

4.9 In addition to securing access to the system and to the data within the system, the PND has extensive auditing systems to deter misuse and, where misuse does happen, to identify and provide evidence against those individuals involved.

4.10 All activity within the PND is logged; this includes all upload of data, both manual and automatic feeds; searches and other data retrieval; reviews and disposals; and administrative activities. These record who did what, when and what results were obtained.

4.11 Whenever users search the system, they also have to enter information saying why they did so and, where appropriate, on whose behalf. This information is also logged.

4.12 In addition to identifying misuse of access rights, the audit service helps to identify attacks on the PND from external sources and from attackers attempting to bypass the system access controls from within. The audit log is 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 of time.

4.13 The log is available to force auditors, who are able to see audit data relating to their force. Auditors 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). PND also offers the capability to support further collaboration between forces in support of audit, allowing auditors from one force access to another force's data with all necessary Data Controller permissions. All activities of auditors on PND are logged and subject to audit.

4.14 The PND Service routinely seeks feedback from auditors on any problems identified so that consideration can be given to the need to strengthen the controls, either through the IT or business processes.

The design of the PND capabilities

4.15 The Police Service can both search and link data on the PND and also analyse it using local intelligence and analysis tools, including exporting it from PND into those tools. There is also analysis functionality within the PND system itself. The ability to export particular data items such as producing electronic or hard copies of individually selected records is also present. A number of measures protect the export processes and any information that has been exported. These include:

- limiting the ability to export large amounts of information
- redaction of information where appropriate
- business rules regarding the use and security of the information
- ensuring the information carries appropriate protective markings
- "watermarking" (to show who exported the information and when it was exported).
- Role Based Access Controls for users' functionality
- Data Access Restriction Codes for users' access to pre-set data Handling Codes
- MOPI RRD functions for data entered directly onto PND.

4.16 The facial search facility was added in 2014; it enables comparison between custody images uploaded onto the PND system from local police force systems and images originating from other sources such as CCTV, mobile phones & cameras and photocopied documents such as passports. The Centre for Applied Science and Technology (CAST) provides advice and guidance to the Home Office, local police forces and other stakeholders on all aspects of the use of facial recognition technology; it works closely with the Home Office Biometrics Programme to provide advice on facial image standards and face recognition technologies and use cases, and with the Forensic Science Regulator on developing new processes and standards for police use of facial images.

4.17 As the facial search capability was added after the introduction of the Code of Practice on Police Use of PND, there is no specific guidance in that document as to its use. However, there are a number of privacy safeguards in place: -

- The matching of images is not entirely automated; the user's human eye is the deciding factor in concluding that two separate photographic images relate to the same subject.
- Authorised users of facial search are trained to use the system correctly and to exercise careful judgement in relation to determining a match.
- Auditing of transactions to identify and deter misuse of the facility.
- The match results are not used for evidential purposes but are treated as intelligence.

4.18 The recent Custody Image Review, carried out by the Home Office in 2016, has recommended a number of measures including:-

- the deletion of the custody images of unconvicted individuals, upon application, on a case-by-case basis, with a presumption that the images of those without convictions will be deleted, in line with APP guidance, unless retention is necessary for a policing purpose.
- for unconvicted individuals whose image was taken when they were under 18 years old, its retention should be only where there is a highly exceptional reason to do so.
- the ability for convicted individuals to apply for the deletion of their custody image after a specified period of time have passed since they were convicted without a presumption of deletion when a review takes place.

The proposed approach balances the need to use information, data and intelligence to protect the public, against the Article 8 rights of individuals.

Data quality and consistency

4.19 Data quality and consistency are important aspects of privacy. These attributes ensure that the PND is an effective system that meets the needs of the Police Service and poor data quality is a potential barrier to this. Data which is incomplete, inconsistent, not meaningful or misinterpreted due to the different ways forces manage their information, can lead to poor decisions, wasted time or missed opportunities.

4.20 The implementation of the Code of Practice on the Management of Police Information helped police forces to ensure that data was collected, recorded, analysed, reviewed and securely disposed of where no longer needed. This is an ongoing requirement as data is constantly being added to, updated or becoming obsolete and so the effective following of the Code of Practice enables individual police forces to maintain good data quality which, in turn, facilitates good data quality within the PND. Work to encourage forces to achieve the highest possible standards in this area is continuing.

4.21 The PND Service also assists forces to ensure that their data is consistent and of a known quality. To achieve this, the LEDS Programme will work with forces to help them develop national standards to which data must conform and which will be implemented. Monitoring and quantifying the quality of information uploaded by forces informed the design of the PND from a data quality perspective. Feeding back information to forces where the data does not meet the standards helps them to drive up quality.

Accuracy of data

4.22 Ensuring that data are up-to-date, accurate, relevant, not excessive, adequate and used fairly are all elements of the 8 data protection principles. However, reviewing each item of information against these criteria before placing it on the PND is not practicable. As PND holds a copy of records already held in force there is an expectation that that this is already done in force. In addition, deciding what is fair, relevant, not excessive and so on depends on the circumstances in which the data will be used, and whether something is accurate and up-to-date can quickly change.

4.23 The responsibility is on users of the system to consider, within the context of the enquiry they are dealing with, whether these criteria are met. In doing so, they need to consider whether it is necessary to contact the force that originally obtained the information to check whether it is still up-to-date and accurate.

4.24 Business Rules ensure that MOPI rules, applied to data on source systems, are also applied to the corresponding data uploaded onto PND. MOPI functionality, relating to Direct Data Entry on PND, ensures that MOPI rules are also applied to such data items.

Victim and witness information

4.25 PND holds some information about victims. The need for, and value of, sharing such information for policing purposes has been considered alongside the potential implications for the privacy of the individual concerned. It has been decided that there is insufficient justification for the creation of Person Records relating to witnesses, on the PND, and that Person Records for victims should only be created where justified (i.e. victim information only from those offences listed in Schedules 3 and 5 of the Sexual Offences Act 2003) This position is based on discussions both within the Police Service and with the Information Commissioner when the initial PND PIA was formulated and is being maintained.

Medical and health information

4.26 There is a necessity for some information about people's health to be placed on the PND so that the Service can, for example, provide adequate care for individuals who are placed in custody or to help safeguard their officers. This information may be supplied as part of the local force records uploaded to PND.

Retention and up-dating of data uploaded to PND

4.27 The PND will contain information which each force has agreed to load onto the system from their own local systems. The information provided by each force is updated on a daily basis, via automated updates although manual updates may also be undertaken. This keeps the data as up-to-date as possible.

4.28 When a force disposes of data from its local system, the copy of that data held on the PND will also be removed. (Any copy of that information held in audit logs will normally be retained but only for use for auditing purposes.)

Openness and transparency

4.29 The Data Protection Act requires, subject to certain exemptions, that data subjects be told what information is held on them and how it is used. It will often not be possible to tell subjects exactly what data is held on them or exactly how it is being used as this could compromise the prevention and detection of crime. It may sometimes not even be possible to tell individuals whether any information is held on them. Personal data held on PND is simply a copy of the personal data held in the local force IT system. The data being held on PND enables access by other law enforcement agencies for a policing purpose. The presence of the information on PND does not change it in any way and it does not change the purpose for which it is held.

4.30 More generally, the Police Service are as open and transparent as possible about the PND.

4.31 Chief Officers are acting as "data controllers in common" for the information on the PND. As such, it has been decided that they all "hold" all the information on the PND that they can access. In responding to subject access requests[5] they must therefore consider all the information on the PND, not just the information provided by their force.

Business rules

4.32 Whilst the PND itself provides a high level of protection for the data, the need for rules around how the system and any information obtained from it are used is recognised. The Home Office has agreed that these take the form of the statutory code of practice with additional and more detailed guidance where required. Chief Officers are legally required to have regard to such codes of practice.

---

[5] Subject to certain exemptions, the Data Protection Act gives data subjects the right of access to details of the information held on them and how it is used.

4.33 The guidance addresses issues including:

- The purpose of the PND and any restrictions on its use;
- Some general concepts, such as the responsibilities of Chief Officers (as “Data Controllers in common”), the need to ensure the system is used in a way that is non-discriminatory, the security of the system and who has access;
- Loading data – including the principles for what information to send / not send, data quality and interpretation, how the requirements relating to the review, retention and disposal of police information apply to the PND, how the linking of information works;
- Using the PND – including searching, administering and auditing, and the vetting and training of users;
- Using the information from the PND – responsibilities for ensuring it is fair, necessary, proportionate, accurate and up-to-date; ensuring information obtained from the system is managed appropriately; disclosure of the information to other agencies; and
- Other matters such as dealing with subject access requests.

4.34 The high level strategy in the form of a code of practice has been published internally.

4.35 Reference documents to be used in conjunction with this PIA are the PND Code of Practice, Manual of Guidance the ACPO/ACPOS Community Security Policy and the Public Sector Network (PSN) Code of Connection.

5 The Police National Computer, its associated processes and privacy concerns

5.1 The PNC holds detailed information on people, including identifying information such as name, age, sex, colour and height, combined with data concerning arrests, charges & court disposals (including convictions) pertaining to those individuals; records are also held of those who hold driving licences (or are disqualified from doing so) or firearms licences. The system also holds information about vehicles such as the identity of the registered keeper and about other types of property. Additionally, it holds alert and warning information about nominals, vehicles and addresses including wanted/missing reports.

5.2 PNC’s capabilities can be described as follows: -

- Names (Nominal Element) is the identifying information such as name, age, sex, colour and height held about individuals who have a nominal record on PNC. Where an individual has supplied or is known to use more than one name, the alternative names are recorded as aliases, but linked to the main nominal record. The information recorded about nominals includes information markers about them such as health conditions or warning markers which contain important information for law enforcement officers or other officials who may come into contact with them. Each

nominal is assigned a unique reference number which is permanently attached to that record.

- Names (DVLA) is a record of all the holders of driving licences within the UK. It is supplied as a file by the DVLA and updated at regular intervals.
- Offences Processing Element comprises data relating to the arrest/ summons, prosecutions, remands in custody and disposals (both by courts such as fines or terms of imprisonment and out of court e.g. cautions). Details of disqualified drivers are also held.
- Vehicle information includes an extract from the DVLA with details of the registered keeper of all vehicles currently registered and which is updated at regular intervals. Reports supplied by police officers record stolen vehicles or those which are of interest due to suspicion of being involved in crime.
- Operational Information includes wanted/missing reports covering individuals who have either been reported as missing from home, have absconded from prison or other lawful custody or are wanted in connection with an offence.
- Broadcasts enables messages to be sent out to all forces with relevant information; the facility also allows them to be cancelled when no longer required.
- Property can also be recorded on PNC, primarily by means of reports concerning stolen property recorded by police forces.
- Details of Firearm certificate holders are held on the PNC together with details of the Firearms they hold.
- Schengen - In the UK officers create, circulate and respond to alerts from the Schengen Information System via the Police National Computer (PNC) in relation to vehicles, property and persons. Within the EU, notifications of convictions on PNC are sent to the country of nationality whilst, on request, the UK provides details of the PNC convictions of UK nationals being prosecuted abroad.
- Other international sharing outside the EU occurs. The National Police Chiefs' Council (NPCC) Association of Chief Police Officers Criminal Records Office (ACRO)[6] sends some conviction notifications to the country of nationality subject to risk assessment based on the conviction type and the country of receipt. Aside from Schengen's automated processes, data can be shared, on a one off request basis, with other countries through the National Crime Agency (NCA)'s Interpol function.

5.3 PNC incorporates a number of features which assist in addressing privacy concerns related to the system:

- the system is only accessible by authorised, vetted and trained users from police or other authorised user organisations;
- most users have read-only access so that they cannot add, change or delete information on the system – such work must be undertaken by specially trained staff.
- all enquiries on the system are pre-formatted and return a limited set of data, relevant to the specific enquiry;
- users are only able to access the type of information and facilities that they need to do their job;
- all use of the system is logged and subject to audit;

[6] Formally ACPO (The Association of Chief Police Officers) <https://www.acro.police.uk/>

- rules for the use of the system, and of any information obtained from it, are set. These include that the system and data must only be used for policing purposes.

Safeguarding access to the system and its data

5.4 PNC holds information classified up to RESTRICTED according to the GPMS which has now been replaced across the public sector outside policing by the Government Security Classification Scheme. It is expected that the new LEDS platform, to which PNC will be migrated in 2018, will be classified as OFFICIAL, possibly with the handling instruction of OFFICIAL-SENSITIVE, but existing markings on data within the PNC system will be maintained.

5.5 The 43 police forces in England and Wales, Police Scotland, British Transport Police, Police Service of Northern Ireland, National Crime Agency, Service Police Crime Bureau, HM Revenue & Customs, Scottish Crime and Drug Enforcement Agency and ACRO have full access to PNC. Some non-police organisations have been granted restricted access to PNC whilst some other organisations are permitted to obtain PNC information indirectly from a connected organisation. The Police National Computer/Databases Information Assessment Panel (PIAP), part of NPCC, is responsible for authorising access to PNC data by non-police agencies upon receipt of a justified business case. This panel is made up of several Police representatives who decide whether the business case submitted by the organisation is acceptable; the access granted to individual organisations is documented in a Supply Agreement which clearly sets out what they can access and the purpose for doing so. A number of these have been in force for some years and might benefit from a review; a process that is planned as part of the migration to LEDS. PNC data is also shared with a small number of external companies such as Experian in connection with hire purchase checks on vehicles and motor insurance information – the information shared is limited to a small subset of relevant data.

5.6 Access to PNC is via a user identity, issued by the local administrator, and a password chosen by the user which requires updating at regular intervals. Accounts which remain dormant for a specific period will be automatically blocked unless reactivated by an administrator. If a user does not access their account for more than 6 months, they will need to be retrained before their account is reactivated.

5.7 Controls determine which PNC transactions (“enquiries”) a user account can access, including the ability to control access to functions such as printing.

5.8 Requests for PNC checks carried out over the air or via telephone require authentication before the information can be provided.

Auditing use of the system

5.9 The PNC has an extensive auditing regime to provide a deterrent against misuse and to identify and provide evidence against those concerned where it does occur. All user activity within the PNC is recorded with all transactions requiring the provision of a reason for carrying it out which is also recorded; this enables the identification of the end requester in transactions carried by an authorised user on behalf of another member of staff.

5.10 The PNC Code of Connection and the PNC Manual mandate that all user organisations must examine a sample of transactions carried out by their users on the PNC system (transaction monitoring) on a regular ongoing basis. Additional proactive audits may be undertaken on an intelligence-led basis, particularly by Anti-Corruption Units (ACUs) within each police force. Police forces also deploy automated monitoring tools which will look for possible misuse including access to PNC from their network.

5.11 Her Majesty’s Inspectorate of Constabulary (HMIC) has undertaken a limited programme of audits of non-police organisations with access to PNC to determine their compliance with their individual Supply Agreements; this was found to be generally

satisfactory. This audit programme could be extended to cover all non-police organisations on an ongoing basis.

5.12 The PNC Service supports local and national forums where any issues identified by users, auditors and local administrators are considered so that consideration can be given to addressing them.

Data quality and consistency

5.13 Data quality and consistency contribute significantly to the privacy of individuals whose data is held on PNC. PNC maintains a generally good data quality regime by limiting the ability to create, modify or delete records manually to the central administration team and to trained staff within the police user organisations. Some data enters the system via uploads from other police or criminal justice systems and the quality of this data is dependent on the data quality at source. The majority of these systems are police owned and are subject to the MOPI Code of Practice, requiring forces to maintain their data to a good standard.

Accuracy of data

5.14 Ensuring that data are up-to-date, accurate, relevant, not excessive, adequate and used fairly are all elements of the 8 data protection principles. Manual updating of the system is carried out by specially trained staff within police forces with further work carried out by central administration teams.

5.15 PNC mandates a data quality audit regime by the organisations which own the data (the police forces are data controllers in common whilst other organisations supplying data have their own data controllers). Auditing is carried out locally by police forces on PNC itself and on other systems which supply data to PNC via interfaces. The system data is checked for compliance with Principles 3 & 4 of the DPA 1998. It is anticipated that this audit regime will continue during and following the transition process to LEDS.

Up-dating of data on PNC

5.16 PNC contains arrest, charge, conviction and caution data placed on the system by each police force; other authorised user organisations will have an arrangement with a police force where they pass their information to the police force PNC Bureau for addition or alteration on PNC. There are also automated updates from police forces and other criminal justice systems on a regular basis, often daily, and this keeps the data as up-to-date as possible.

5.17 Further work is carried out by central teams to merge or rename files; they can also repair any records which have been identified as being corrupted in some way.

5.18 Automated deletion of information with a weed date such as driver disqualifications also occurs.

Other personal data

Victim information

5.19 PNC holds some information about victims relating to those who are the subject of protective orders (e.g. Domestic Abuse Prevention Orders). This processing is intended to benefit the victims by making information about the protective orders available to officers in a timely manner to enable their enforcement. PNC also holds details of missing persons although these are not necessarily victims of crime.

5.20 The need for, and value of, sharing such information for policing purposes has been considered alongside the potential implications for the privacy of the individuals concerned. It is felt that the safeguarding benefit to the victim is paramount.

Medical and health information

5.21 There is a necessity for some information about people's health to be placed on the PNC so that the police service can, for example, provide adequate care for individuals who are placed in custody or to help safeguard their officers. This information is added by individual forces where considered relevant and necessary.

Non-crime related information

5.22 PNC holds an extract from the DVLA Drivers' Database, a record of every driving license holder in the UK including disqualifications, endorsements and driving restrictions (which may include some relevant medical information). An extract of the DVLA Vehicles Database is also held, recording details of every vehicle registered in the UK including its registered keeper. This information is supplied by the DVLA under an agreement with the Home Office and the data extracts are updated at regular intervals. Motor insurance information supplied by the Motor Insurers' Bureau is also present on the system. All of this information is updated at regular intervals. Similarly, information is held about individuals who hold or have held firearms licences.

5.23 The volume of records involved is substantial; there are around 55.4 million driver records and 54.8 million vehicle records whilst there are approximately 10.7 million criminal records, thus non-criminal records form a substantial part of the PNC. Whilst the processing of personal data about millions of individuals with no criminal links on a database whose primary purpose is to support policing objectives such as the detection of crime could be seen as potentially prejudicial to them, access to this information is limited to those who need to know for a policing purpose.

5.24 The need for, and value of, sharing such information for policing purposes has been considered alongside the potential implications for the privacy of the individual concerned. Enabling law enforcement to quickly identify vehicle ownership, driving entitlement and the existence of valid motor insurance in a variety of policing situations provides benefits to society including those individuals whose personal data is being processed.

Retention

5.25 The PNC retention period differs from the MOPI mandated retention periods for data held on PND. Personal data, conviction details and the associated fingerprints and DNA profile will, for an adult convicted (including cautioned) for a recordable offence, be retained until the person's 100th birthday. Lesser retention periods apply for juveniles convicted of minor offences. Retention of biometrics is also possible for limited periods for individuals charged with more serious offences and in rare cases, limited period retention is possible for people arrested but not charged with the most serious offences. Arrest data will be retained in all cases, ie including conviction and non-conviction arrests although the Protection of Freedoms Act 2012 makes provision for individuals to apply for the deletion of their data in specified circumstances (e.g. no crime, malicious/false allegation). Any such applications are made directly to the Data Controller of the police force which owns the nominal record concerned and any deletion of data is at their discretion. The retention period for arrest, conviction and caution data has been subject to legal challenge in the past but was confirmed by the Court of Appeal in 2009.[7]

5.26 Nevertheless it is recognised that the retention of information concerning those arrested but not charged or who are charged but subsequently not convicted of any offence and who have no previous convictions recorded could be seen as disproportionate in the context of data protection as could the retention of a number of old records relating to individuals with a small number of historical minor offences with no recurrence which have been retained in line with current rules. The retention of the arrest only records is currently under review with

[7] Chief Constable of Humberside v Information Commissioner & Another [2009] EWCA Civ 1079

consideration being given to the removal of a number of such records from the system whilst ensuring that records relevant for a policing purpose are retained.

Openness and transparency

5.27 The Data Protection Act requires, subject to certain exemptions, that data subjects be told what information is held on them and how it is used. It will often not be possible to tell subjects exactly what data is held on them or exactly how it is being used as this could compromise the prevention and detection of crime. Sometimes it may be necessary to neither confirm nor deny that information is held. The data held on PNC enables access by police forces and other authorised organisations to defined datasets for a policing purpose.

Business rules

5.28 Use of PNC is governed by the Code of Connection with which all user organisations must comply, together with the PNC Manual of Guidance and other published guidance. Non-police organisations are required to comply with their Supply Agreements which also require that they develop Security Operating Procedures.

5.29 Reference documents to be used in conjunction with this assessment are the PNC Code of Connection, the Manual of Guidance, the ACPO/ACPOS Community Security Policy and the Public Sector Network (PSN) Code of Connection.

6 The Law Enforcement Data Service (LEDS) and its associated privacy concerns

6.1 The Law Enforcement Data Service (LEDS) will bring together information currently held in silos across a number of national systems onto a single platform where it will be linked and, where possible, matched. NB there is no intention to merge the two data sets. The intention is instead to enable authorised users within UK law enforcement and other largely public protection agencies to access data from the systems on the platform through a single search rather than conducting enquiries on the individual systems as now.

6.2 LEDS' intended capabilities can be described as follows: -

- A platform which supports the primary law enforcement systems (PND initially, followed by PNC with the likelihood of other systems being added in the future).
- A single point of access for law enforcement agencies and trusted partners to joined up person/object centric data sets with the intention that more organisations will have direct access to information where it is appropriate for them to do so.
- Enhanced search and data matching capabilities
- Providing new insights that better support crime prevention and public safeguarding
- Making data available closer to real time
- Developing clear data sharing agreements
- Delivering services at the point of need
- Maintaining continuity of service.

6.3 The intention is for LEDS to incorporate a number of features which will address privacy concerns:

- the LEDS capabilities are being designed with full consideration of privacy requirements (privacy by design);
- the systems located on the platform will only be accessible to authorised, vetted and trained users from police or other authorised user organisations;
- users will only be able to access the types of information and facilities that they need to do their job;
- all use of the platform and its systems will be logged and subject to audit;
- rules for the use of the platform, its systems and of any information obtained from them will be designed. These will include specifying that the system and data must only be used for policing purposes.

Safeguarding access to the system and its data

6.4 It is expected that the new LEDS platform will be classified as OFFICIAL in line with the Government Security Classification Scheme, possibly with the handling instruction of OFFICIAL-SENSITIVE, but existing markings on data within the PNC and PND systems will be maintained. The LEDS system will hold data from both systems, the vast majority of

which is classified as RESTRICTED according to the GPMS. Around one per cent of the information originating from the PND system is classified as CONFIDENTIAL under GPMS and will require adequate security measures to ensure that it is accessible only by authorised individuals; this is particularly important in view of the increased number of non-police user organisations which may have access to the platform and thus potential access to PND data; the increasing use of mobile data is also a consideration in this context.

6.5 As with the existing systems, the primary user organisations of the systems on the LEDS platform will comprise the 43 police forces in England and Wales, Police Scotland, British Transport Police, Police Service of Northern Ireland, the National Crime Agency, the Disclosure and Barring Service, the Service Police Crime Bureau, the Scottish Crime and Drug Enforcement Agency and the National Police Chiefs' Council (ACRO). There are a number of non-police organisations with access to PNC data, whether directly to a limited set of "enquiries" or indirectly from a connected organisation whilst a small but increasing number of non-police organisations are being granted access to PND; each system has its own supervising body which considers and approves applications for access to the system in general or to particular datasets. Going forward, consideration could be given to development of a new overarching governance model which would incorporate provision for the consideration of external applications to access data on LEDS. This could also provide the opportunity to review existing access by non-police organisations, looking at the proportionality and necessity of their access to specific data classes.

6.6 The move onto LEDS will necessitate consideration of an appropriate access and authentication mechanism for users. At present, PNC and PND utilise two different authentication mechanisms (IAM for PND and username & password for PNC). In view of the sensitivity of a small proportion of the data on PND, and making use of an opportunity to enhance security controls around all PND & PNC data, the implementation of IAM across the entire platform could be considered. This would remove the reliance on less secure user passwords that can be compromised or shared and would help ensure that that users are identifiable when they access the system directly. IAM would also assist in ensuring that any use of the PND can be traced through a rigorous and secure auditing process. This may lead to a greater management overhead due to the issuing process required for a much larger user population on LEDS than currently exists for PND but this could be balanced against the improved security for all data on the platform.

Safeguarding access to the data and LEDS capabilities

6.7 IAM also supports RBAC (Role-Based Access Control) which ensures that users only have access to capabilities and information that they need for their business role. Attribute-Based Access Controls are also being designed into the solution to further limit the access to data and system functions granted to a user account. So for example an officer in the Disclosure and Barring Service whose role concerns the disclosure of criminal convictions would only have access to criminal convictions held on LEDS. An example of Attribute Based Access Controls would relate to the police; specific attributes relating, for example, to counter-terrorism would only be accessible to a limited number of officers.

Transfer of data onto LEDS

6.8 Once the LEDS platform has been constructed, individual systems will be migrated onto it. The migration processes have been designed to enable the systems to keep running with minimal interruption to user services whilst maintaining the integrity and confidentiality of the data.

6.9 PND Data Transition will cover the migration of data held in PND (synchronisation) and daily feeds (interception); synchronisation will process both operational and non-operational data currently held in PND and interception will capture existing PND updategrams, routing them to the LEDS environment to be pre-processed and loaded into LEDS.

6.10 For PNC, it is planned that the entire database will be replicated with information being updated on both the live replicated system on LEDS and the legacy system, with ongoing comparison between them to ensure accuracy prior to the final switchover to LEDS. Only when the project team is satisfied that the data in the LEDS iteration is accurate against the legacy system will the final switchover to the LEDS platform take place. As part of this work, data analysts will undertake analysis of the data contained on the live database. It is recognised that this goes against normal practice and presents a risk to the privacy of individuals whose details are held on PNC as the analysts will have access to data which would otherwise normally be accessible only by those with a policing purpose to do so; there is also a danger that the analysts may alter the data. To address these concerns, experienced analysts who have been trained and vetted will be deployed and all activity will be monitored and audited.

6.11 Once migration has been successfully completed with system functionality and data integrity on the platform confirmed, the legacy systems will be decommissioned and all data deleted or disposed of securely.

Co-location of data on LEDS

6.12 Consideration is being given to the relationship of the data on the platform i.e. whether the data pools for PNC and PND should be merged on the system or whether separation should be maintained whilst still enabling a single search to bring back data from both systems. In their current form, each system has its own processes in areas such as data management and retention which differ from each other. There are also different user organisations accessing each system in addition to the core law enforcement users. Any decision to merge PNC and PND data will be subject to a further PIA.

6.13 One significant change will be the suggested deployment of a less formalised search facility across the platform. This will represent a significant development in the search capability for current PNC users compared to the “enquiries” which return a clearly defined dataset in response to a predefined enquiry. It could result in less but more specific information being returned in relation to a search but it could also result in additional information being returned which was not previously available. This could include intelligence data from PND to which organisations with PNC access only are not currently privy and which their users are not trained to interpret. To address this risk, the project team propose the deployment of both Role-Based Access Controls (RBAC) and Attribute-Based Access Controls (ABAC) to limit access to data to that which the user needs and is relevant to their role. This will usually be done by not reporting the hit to the user.

The design of the LEDS capabilities

6.15 The Police Service requires the ability to search and link the data that will be on LEDS, and to able to analyse it using intelligence tools. The capabilities and facilities which currently exist on both PND and PNC are expected to be carried onto the LEDS platform although the development of a search capability across the entire platform which will replace the existing “enquiries” on PNC will represent a substantial enhancement for PNC users. The platform design will take account of the existing measures in place to protect the export processes and any information that has been exported such as limitations on the ability to export large volumes of information, redaction of information where appropriate, “watermarking” of information to show the source and the use of business rules regarding the use and security of the information, developing and enhancing these measures where required.

Data quality and consistency

6.16 Data quality and consistency are important features of any system and are being given due prominence in the design of LEDS. PNC currently has a generally good data quality regime and this should be maintained during and following migration to LEDS.

6.17 Management of PND data follows the MOPI Code of Practice which provides effective guidance to police forces concerning the collection, recording, analysis, review and secure disposal of police data on an ongoing basis. This requires forces to apply the guidance effectively at local level as poor data quality locally will be reflected in the records uploaded to PND. Work to encourage forces to achieve the highest possible standards in this area is ongoing.

6.18 To ensure that data on the LEDS platform, whatever its origin, is consistent and of a known quality, the NLEDP will work with forces to help them develop national standards, to which data must conform, for implementation either before or after migration to LEDS, subject to time and other constraints. Monitoring and assessing of the quality of information on LEDS will be carried out, with the results being fed back to forces where the data does not meet the standards to help them to drive up quality.

Accuracy of data

6.19 Ensuring that personal data complies with the Third and Fourth Data Principles i.e. it is adequate, relevant and not excessive, and that it is accurate and kept up to date is an important part of the data management required for LEDS. Merging the PNC and PND data pools might present difficulties in adhering to these principles. It is recognised that the accessibility of the entire combined data pool to users from partner organisations, particularly those with no previous exposure to PND data, might lead to those users having access to data which is excessive and not relevant; the design process being followed includes development of suitable controls to limit the access to data and facilities to that which is relevant to both the organisation and the user's role. This could be supplemented by a governance regime which restricts access to LEDS to only that which is necessary and proportionate.

6.20 If the PNC and PND data pools are merged, this could also lead to conflicts internally between the data about an individual supplied from the different primary sources; there are also differences in the way that data is updated on each system. Inability to identify the source of data could make it difficult to maintain the data as accurate and up to date, particularly where the origin of a specific record, or individual items of personal data thereon, cannot be attributed to a particular user organisation. This could lead to a situation where the accuracy of the data cannot be verified or it is not updated in a timely fashion with a potentially adverse impact on individual privacy and operational policing. Co-location but continued separation of the PNC & PND data pools would mitigate this.

Retention

6.21 As described earlier in this report, PNC and PND operate two different data retention regimes. The PNC data retention regime is under review in relation to the retention of information concerning those arrested but not charged, those who are charged but subsequently not convicted of any offence and who have no previous convictions recorded could be seen as disproportionate in the context of data protection. Proposals are being considered to delete a number of records which meet these criteria whilst ensuring that records relevant for a policing purpose are retained. Any such deletion would be likely to occur following the migration of PNC data to LEDS due to the scale of the work required and the time constraints.

6.22 The move to place both PNC and PND on LEDS may be an opportunity to devise a single retention regime, based upon the MOPI Code of Practice, for application to all police data on the platform. MOPI requires the review of police data at regular intervals as defined in the Code of Practice, depending on the nature of the offence concerned, with data being

securely deleted when no longer required. If this were followed, PNC arrest, charging and conviction data would be reviewed in line with MOPI and many minor offences would be reviewed and considered for deletion at earlier and more regular intervals compared to the current regime. Provision could be made for elements of the existing PNC regime relating to areas such as warrants, wanted missing, warnings and markers to be incorporated into any new retention regime.

Victim information

6.23 It is anticipated that victim information will be processed on the LEDS system in line with the current situations on PND and PNC i.e. victim information from those offences listed in Schedules 3 and 5 of the Sexual Offences Act 2003 (PND) and information relating to those who are the subject of protective orders on PNC (e.g. Domestic Abuse Prevention Orders). A continuing need for, and value in, sharing such information for policing purposes has been identified; the potential implications for the privacy of the individual concerned have also been considered. Discussions with the Information Commissioner during the formulation of this PIA indicate that this is an appropriate position. It is recognized that more organisations will be granted access to the data on the platform than is currently the case for PND or the victim data on PNC and that suitable security measures will be required to ensure that access to victim data is tightly controlled, given its sensitivity.

Medical and health information

6.24 As with the existing PND & PNC systems, there is a necessity for some information about people's health to be held on LEDS so that police forces can provide sufficient care for individuals taken into custody or to enable the wider range of user organisations to help safeguard their staff who may come into contact in a professional capacity with the individuals concerned. The information will continue to be added by individual forces where considered relevant and necessary. Care will be taken to ensure that all access to this data is restricted to those for whom access is necessary and proportionate.

Non-crime related information

6.25 LEDS is expected to hold the same datasets which comprise the current PNC system including the extracts from the DVLA Drivers' Database and the DVLA Vehicles Database and the motor insurance information supplied by the Motor Insurers' Bureau. Firearms licencing information will also be processed. All will continue to be updated at regular intervals.

6.26 This information will be available to search on the platform alongside the intelligence data held in the PND system and it could be seen as potentially prejudicial to the millions of individuals with no criminal links whose data may be returned from a search alongside intelligence about individuals of police interest. Access controls will put in place to ensure that access to this information will be limited to those who need to know for a policing purpose.

6.27 The need for, and value of, sharing such information for policing purposes has been considered alongside the potential implications for the privacy of the individuals concerned. Enabling law enforcement to quickly identify vehicle ownership, driving entitlement and the existence of valid motor insurance in a variety of policing situations provides benefits to society including those individuals whose personal data is being processed.

Auditing use of the system

6.28 Both PND and PNC have effective ongoing audit regimes which operate primarily on a retroactive basis. Going forward, all activity carried out on the LEDS platform by users, administrators, developers and support staff will be logged. As with the existing systems, this will include any addition to or amendment of data on the platform, (whether manually or from automated feeds), searches and other data retrieval; reviews and disposals and

administrative activities. The logs will record the actions carried out, by whom and when, the purpose for carrying out any search and the results obtained; users must also identify any person on whose behalf they carried out a search where appropriate and this information is also logged.

6.29 The audit data recorded will also assist in identifying attacks on the LEDS platform from external sources and from attackers attempting to bypass the system access controls from within. This will form part of a wider protective monitoring regime which will be deployed on LEDS.

6.30 The audit regime will require both reactive (i.e. investigating where misuse is suspected) and proactive audits (i.e. random sampling of all activities to check for misuse).

The audit log will be used for the purposes of:

- proving the integrity of the transactional data to support evidential disclosure of fact-based data on LEDS; and
- monitoring LEDS for improper use, including analysing patterns of usage over a period of time.

6.31 Auditors will be able to provide feedback on any matters identified so that consideration can be given to the need to strengthen the controls, either through the IT or business processes.

Openness and transparency

6.32 The Data Protection Act requires, subject to certain exemptions, that data subjects be told what information is held on them and how it is used. It will often not be possible to tell subjects exactly what data is held on them or exactly how it is being used as this could compromise the prevention and detection of crime. Sometimes it may be necessary to neither confirm nor deny that information is held. The data to be held on LEDS enables access by police forces and other authorised organisations to defined datasets for a policing purpose.

6.33 A more general engagement with public and press to explain the purpose and benefits of the LEDS platform and the systems it will host, such as their role in safeguarding the vulnerable, could lead to increased public confidence concerning the processing of their personal data by the Police Service and other stakeholders.

Business rules and Governance

6.34 Both PNC and PND have effective governance arrangements in place at the current time and it is anticipated that these will continue to operate as normal for the time being.

6.35 The NLEDP has a governance structure in place including a Business Design Authority for the approval of design decisions and deliverables during the development of LEDS.

6.36 Going forward, consideration is being given to the development of an overarching governance structure for all data on the platform. This could cover a number of areas including, but not limited to: data ownership, responsibilities for data management and compliance with data protection requirements (including subject access requests), system administration, the granting and management of access rights for both organisations and users, information sharing and the development of data quality standards.

6.37 In particular, the governance arrangements could include reviewing and applying clear criteria for organisations to be granted access to LEDS, the purposes for which they may use it and the role profiles available to their users; review of existing agreements could also be carried out.

7. Findings and recommendations

7.1 The supervisory bodies for the PND and PNC systems are actively working together, and will continue to do so, to ensure that the manner in which these systems are used are as privacy-friendly as possible. Similar consideration is being given to the development of the LEDS platform onto which it is planned that these systems will be relocated within the next two to three years.

7.2 Further work, including ongoing consultations with stakeholders and other interested parties such as the Information Commissioner's Office will be carried out to ensure the potential impacts on privacy are identified and fully considered in designing, implementing and using the LEDS platform and the data which will be processed on it.

7.3 The PND system addressed many privacy issues during the course of its development and introduction into service as evidenced in the 2013 iteration of the PND PIA. Further to this, the following suggested measures could enhance privacy: -

- Implementation of the measures recommended in the Custody Images Review, published by the Home Office in February 2017.
- A data quality improvement exercise, possibly targeted at specific areas where some work could produce a substantial improvement in data quality.

7.4 In relation to PNC, this system has many effective measures in place to safeguard individual privacy. In addition, the implementation of proposals currently under consideration for a weeding exercise on the system to remove old minor arrest and conviction data whose retention is considered excessive whilst retaining data which is relevant for a policing purpose would address concerns which have been identified.

7.5 The NLEDP can address privacy in the way in which the LEDS platform is designed and built, incorporating "privacy by design", and the way in which its supplier operates it. The Programme also has a part to play in establishing the necessary business rules and governance around access to, and use of, the platform. The following measures could be adopted to enhance privacy protection: -

- Maintenance of separation between the PND and PNC data pools.
- Implementation of RBAC and ABAC controls to restrict the data accessible by users and mobile devices
- Development of a strong governance model to include effective management of data and of access by non-police organisations to the data and facilities on the LEDS platform.
- Clear requirements covering data protection issues such as security and privacy to be included in any contracts for the design, building or maintenance of LEDS by third party suppliers.
- Development of a robust audit regime, both proactive and reactive, which includes automated monitoring as required.
- Engagement with the public to increase awareness of the benefits to public safety of the LEDS platform and of the efforts made to safeguard individual privacy during the processing of the data.

7.6 Forces also have a key part to play in ensuring that they use the platform, and the data obtained from it, appropriately. This is ultimately the responsibility of the Chief Officer. NLEDP will liaise with police representatives to develop and promote suitable privacy protective measures.

8. Review and audit

8.1 The purpose of the “Review and audit phase” of a PIA is to check whether the actual impacts on privacy are those that were anticipated and that the actions that emerged from the PIA have been taken forward and are having the expected effects. Where either is not the case, it allows further action to be taken to assess the impacts and to take appropriate additional action as necessary.

8.2 Impact on privacy will be something that the NLEDP will continue to consider at all stages as the programme progresses. It is anticipated that reviews will be conducted on an annual basis.

Annex A - PIA screening questions & answers for the Police National Database

Questions and Guidance Notes	Response
PIA already conducted	
1. *Has a PIA that relates to this proposal already been conducted?* *If yes, please provide details (e.g. date, whether the PIA was full scale or small scale) and consult the authority for the system before proceeding further with this questionnaire.*	Yes – A full scale PIA was conducted on PND during the project phase in 2009 with a draft and unreleased update in 2013.
Technology	
2. *Does the proposal apply new or additional information technologies (IT) that have substantial potential for intrusion into an individual's personal data?* *Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*	Yes PND now offers a facial recognition function, in that it will, at the request of a user, compare an image introduced to the system with its database of images to search on and find one or a number of possible facial matches. Additionally, PND & PNC data will be co-located on a new LEDS platform, enabling data matching and thus returning increased information from a search of the systems on the new platform.
3. *Does the proposal involve new technologies or technologies that are inherently invasive in relation to an individual's personal data?* *Examples of technologies are as listed in question 2.* *Technologies that are inherently intrusive and technologies that are new and sound threatening, excite considerable public concern, and hence represent a project risk. Things to consider in answering this question include:* a. *Whether all the IT to be applied in the project are already well-understood by the public;* b. *Whether their privacy impacts are well-understood by the organisation and by the public;*	Yes For PND currently, what is specifically invasive about the system is that images of arrested individuals, including some who may have been released due to their innocence, or who may have committed a very minor offence, may not be reviewed in accordance with the judgement of R (RMC & FJ) v Metropolitan Police Commissioner – 22/06/2012 Re LEDS, the new platform will house a number of police systems, enabling data matching across those systems internally rather than requiring users to collate data manually as at present. The public could view this development as being intrusive into their privacy, potentially damaging their trust in Government and law enforcement. Additionally, the platform is likely to be hosted in a cloud environment not owned by the Home Office or Police Service. There is probably limited understanding

Questions and Guidance Notes	Response
c. *Whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected; and* d. *Whether all of those measures are being applied in the design of the project.*	amongst the public about cloud computing They may be uncomfortable with the idea of an external host and may have concerns about possible access to this data.
Identity	
4. Does the proposal involve: *a. An additional use of an existing identifier?* *b. Use of a new identifier for multiple purposes?* *c. New or substantially changed identity authentication requirements that may be intrusive or onerous?* *The public understands that an identifier enables an organisation to collate data about an individual, and identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.*	Yes The use of Facial Search can be seen as an additional use of an existing identifier. Custody pictures are matched with images from other sources such as CCTV – the final determination of a possible match is by human eye. There will be enhanced data matching capability with co-location of the PNC & PND systems on the same platform. An objective of LEDS is to provide a single search capability for both operational information & intelligence from PND and conviction and other data relating to individuals and vehicles on PNC.
5. Might the proposal have the effect of: *a. denying anonymity and pseudonymity, or* *b. converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?* *Many agency functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.*	Yes Details of informants are at risk of being disclosed if data is shared with or accessible to users who are not suitably trained, contrary to the handling rules that form part of the National Intelligence Model. The co-location of PND & PNC on the same platform to link information could help to identify where information might have come from, potentially placing the individuals who provided it at risk. It will be important to ensure that access to a nominal record the co-location of data does not reveal information about an individual in one context does not reveal information about that individual in another context where this would be prejudicial In some cases, police officers may need to keep their identity safeguarded and provide information anonymously - for example, undercover officers, test purchase officers, and officers involved in combating terrorism. Facial search provides the capability to identify more individuals who might otherwise remain anonymous. This is likely to be carried out for a policing purpose but there is the possibility of function creep or of misuse by authorised users. The broadening of access likely to result from the addition of PNC users to the platform

Questions and Guidance Notes	Response
	with potential access to this facility might increase the use of facial search.
Justification	
6. *Is the justification for the new data-handling unclear or unpublished? If yes, why is this the case? Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed for 'security reasons' or 'to prevent fraud' are much less likely to calm public disquiet.*	Yes A High Court ruling in 2012 ruled that two people's data must be removed from a local Metropolitan Police Service system. Forces were reminded by the judge to amend practices within months of the ruling. The Home Office conducted a review of Custody Images in 2016-17, publishing a report on 24 February 2017. Re LEDS, the justification is currently unpublished although the project is in an early stage and the ICO has been made aware of the proposal. However, there is a strong case to be made to the public regarding improved identification and management of offenders, prevention and detection of crime etc.; a degree of transparency regarding the project could reassure the public about the processing of this data.
Multiple Organisations	
7. *Does the proposal involve multiple organisations, whether they are:* *a. government agencies (e.g. in 'joined-up government' initiatives), or* *b. private sector organisations (e.g. as outsourced service providers or as 'business partners')?* *Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.*	Yes PND is a national police system, this involves users from all UK Police Forces, non-Home Office Police Forces, the UK Border Agency and the Disclosure & Barring Service. A number of other organisations such as HMRC will also shortly be gaining access to the system. When moved to the LEDS Platform, PND will subsequently be joined by PNC which has a much larger pool of user organisations across the public sector. The intention is to enable searching of the entire data pool via a single free form enquiry ("Google-type") and this may enable a wider pool of users to access PND data. No decision has been made yet as to whether both systems' data will be housed together or whether they will be physically or logically separate. Care needs to be taken to ensure that, where appropriate, the existence of a record is hidden as opposed to hiding the contents of the record. Allowing access to the data on the platform by a wider range of organisations than is currently the case could impact on the privacy of individuals, particularly where it becomes possible to match data from numerous sources and collate a broader range of data about an individual via the system. This may be desirable from a policing perspective but may also lead to greater insights into the lives of some individuals who are only peripheral to police interest and which adversely impacts upon their privacy.
Data	
8. *Does the proposal involve new or significantly changed handling of:*	Yes The PND data will be moved onto the LEDS platform, to be joined by PNC data. The capability to search across

Questions and Guidance Notes	Response
a. *Personal data that is of particular concern to individuals?* b. *A considerable amount of personal data about each individual in any database?* c. *Personal data about a large number of individuals?* *The Data Protection Act (s.2) identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.* *There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.* *Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.* *Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.* *Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.*	both data sources (and any others added in the future) is an integral part of the proposed platform. Both systems contain very large volumes of sensitive personal data and are the main data sources used by the police service. The information contained on the systems includes data which could locate individuals, sensitive information about their health status, details of arrests, prosecutions, convictions and cautions, warnings etc. Many people may not realise that their data is collected or handled on this scale and may be concerned. The LEDS platform will provide the capability to match data from both systems (and with any other systems added to the LEDS platform subsequently). Re facial search on PND, the particular concern is that some of the data held may be of individuals who have not been found guilty of any crime and that there may be little or no sound* justification for retaining the information.
9. *Will the proposal result in the handling of:* a. *A significant amount of new personal data about each person, or significant change in existing data-holdings?* b. *New personal data about a significant number of people or a significant change in the population coverage?*	The types and volumes of data held on LEDS are likely to remain consistent with current levels but the project hopes to make the processing of the data more efficient and effective. While the current proposal does not involve the capture of more data sets it is acknowledged that co-locating the data would appear to create more data than currently exists in PNC and PNC running separately.
10. *Does the proposal involve new or significantly changed:* a. *consolidation,* b. *inter-linking,* c. *cross-referencing, or* d. *matching of personal data from multiple sources?* *This is an especially important factor. Issues arise in relation to data quality,*	Yes The primary purpose of the LEDS project is to enhance the search capability across the diverse systems and enable a single search to examine all data sources on the platform subject to the data access rights granted the individual user. Data quality on PNC is generally good but PND information is more variable in quality. There are potential data matching issues between the different records held about an individual

Questions and Guidance Notes	Response
the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.	On PND as is, the recent added capability to match facial images captured by a Police Officer on duty or by CCTV to those previously captured during the arrest process involves the matching of personal data from multiple sources.
11. *Does the proposal involve:* a. *New linkage of personal data with data in other collections or* b. *A significant change in data linkages?* *The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called 'front-end verification'), and the matching of personal data from multiple sources.*	Yes The intention is that the enhanced search capability provided when the two systems are co-located on the same platform will enhance the ability to link together records. Although both PNC and PND will be housed on the same platform, it has not yet been determined whether there will be a single data pool or whether the data belonging to each system will be physically or logically separated on the platform. Each system already uses similar identifiers which assist in data matching/linkage.
Data handling	
12. *Does the proposal involve new or changed:* a. *Data collection policies or practices that may be unclear or intrusive?* b. *Quality assurance processes and standards that may be unclear or unsatisfactory?* c. *Security arrangements that may be unclear or unsatisfactory?* d. *Access or disclosure arrangements that may be unclear or permissive?* e. *Data retention arrangements that may be unclear or extensive?*	Yes Facial images may be acquired from CCTV or other sources for comparison with existing images on PND. Many of these images may be acquired without the consent of the subject and in circumstances where they may not be aware that their image has been captured so there may be a fair & lawful processing issue. This might be addressed by the S29 exemption depending on the circumstances but not in every case. Data quality is also potentially an issue. Forces often have a data quality issue on their operational systems. Add to that the reliability of facial search as an image matching tool (variable depending on source of data) and quality assurance could be relevant. Re LEDS, a potential conflict in data retention arises. PNC conviction data is held until the subject's 100th birthday whereas PND follows MOPI with some data being removed at much shorter intervals. This might suggest that it would be advisable to keep the data pools logically separate.
13. *Does the proposal involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?*	No
Exemptions and exceptions	
14. *Does the proposal relate to data processing which is in any way exempt*	Yes

Questions and Guidance Notes	Response
from legislative data protection measures? *Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.*	The systems concerned process data for law enforcement purposes. In general this will fall within section 29 of DPA 1998 though noting that the s29 exemption only provides an exemption from certain parts of the DPA, to the extent that compliance with those parts will prejudice a law enforcement purpose. Processing which is not prejudicial to that purpose is not exempt.
15. *Does the proposal's justification include significant contributions to public security measures?* *Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.*	Yes On PND, the facial search software reduces the time that a Police Officer could spend searching through potential facial matches, compared to the potential hours or days which were previously more realistic. The time-factor often previously discounted this type of analysis. On LEDS, improved search and data matching capabilities will enable law enforcement to build up better and more detailed profiles of nominals and organised criminal gangs and thus improve risk assessment in relation to the likelihood of their committing crime, particularly violent crime.
16. *Does the proposal involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable data protection regulation? Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contactors.* *Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions, such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the UK which are subsidiaries of organisations headquartered outside the UK.*	No
17. *Will the proposal give rise to new or changed data-handling that is in any way exempt from legislative data protection measures?*	No

Annex B - PIA screening questions & answers for the Police National Computer

Questions and Guidance Notes	Response
PIA already conducted	
1. *Has a PIA that relates to this proposal already been conducted?* *If yes, please provide details (e.g. date, whether the PIA was full scale or small scale) and consult the authority for the system before proceeding further with this questionnaire.*	No
Technology	
2. *Does the proposal apply new or additional information technologies (IT) that have substantial potential for intrusion into an individual's personal data?* *Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.*	Yes The data will be co-located on a new platform, enabling data matching and thus returning increased information from a search of the systems on the new platform.
3. *Does the proposal involve new technologies or technologies that are inherently invasive in relation to an individual's personal data?* *Examples of technologies are as listed in question 2. Technologies that are inherently intrusive and technologies that are new and sound threatening, excite considerable public concern, and hence represent a project risk. Things to consider in answering this question include:* a. *Whether all the IT to be applied in the project are already well-understood by the public;* b. *Whether their privacy impacts are well-understood by the organisation and by the public;* c. *Whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected; and* d. *Whether all of those measures are being applied in the design of the project.*	Yes The new platform will house a number of police systems, enabling data matching across those systems internally rather than requiring users to collate data manually as at present. It may also present greater opportunities for information-sharing across the public sector. The public could view this development as being intrusive into their privacy, potentially damaging their trust in Government and law enforcement. Additionally, the platform is likely to be hosted in a cloud environment not owned by the Home Office or Police Service. There is probably limited understanding amongst the public about cloud computing They may be uncomfortable with the idea of an external host and may have

Questions and Guidance Notes	Response
	concerns about possible access to this data.
Identity	
4. *Does the proposal involve:* a. *An additional use of an existing identifier?* b. *Use of a new identifier for multiple purposes?* c. *New or substantially changed identity authentication requirements that may be intrusive or onerous?* *The public understands that an identifier enables an organisation to collate data about an individual, and identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.*	Yes There will be enhanced data matching capability with co-location of the PNC & PND systems on the same platform. PNC may also gain enhanced data processing capabilities. Currently it is limited to processing text only but the new platform and user interface may enable the processing of additional types of data such as photographs This could provide greater opportunities for facial search/matching.
5. *Might the proposal have the effect of:* a. *denying anonymity and pseudonymity, or* b. *converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?* *Many agency functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.*	No The data is solely for law enforcement use. PNC already contains alias information concerning nominals who use more than one name. Provision for access by Home Office statisticians to depersonalised data should be made.
Justification	
6. *Is the justification for the new data-handling unclear or unpublished?* *If yes, why is this the case?* *Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed for 'security reasons' or 'to prevent fraud' are much less likely to calm public disquiet.*	Yes The justification is currently unpublished although the project is in an early stage and the ICO has been made aware of the proposal. However, there is a strong case to be made to the public regarding improved identification and management of offenders, prevention and detection of crime etc.; the benefits to enhancing public safety can be demonstrated.
Multiple Organisations	
7. *Does the proposal involve multiple organisations, whether they are:* a. *government agencies (e.g. in 'joined-up government' initiatives), or* b. *private sector organisations (e.g. as outsourced service providers or as 'business partners')?*	Yes PNC data is owned and used by UK police forces and a number of other law enforcement & public sector agencies and initially this is unlikely to change. The project provides an opportunity to review

Questions and Guidance Notes	Response
Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.	access to the data by other organisations and to assess the appropriateness of that access and whether it complies with the policing purpose. The existing system is housed on a mainframe at Hendon Data Centre owned by the Home Office but the expectation is that, when the data is replicated and moved onto the LEDS platform, it will be hosted by an external provider, possibly from the commercial sector. Relevant security measures (technical & organisational) will be required to protect the data.
Data	
8. *Does the proposal involve new or significantly changed handling of:* a. *Personal data that is of particular concern to individuals?* b. *A considerable amount of personal data about each individual in any database?* c. *Personal data about a large number of individuals?* *The Data Protection Act (s.2) identifies a number of categories of 'sensitive personal data' that require special care.* *These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.* *There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.* *Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.* *Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.* *Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.*	Yes The PNC data will be moved onto the LEDS platform to join the PND data which will already be located there. The capability to search across both data sources (and any others added in the future) is an integral part of the proposed platform. Both systems contain very large volumes of sensitive personal data and are the main data sources used by the police service. The information contained on the systems includes data which could locate individuals, sensitive information about their health status, details of arrests, prosecutions, convictions and cautions, warnings etc.
9. *Will the proposal result in the handling of:* a. *A significant amount of new personal data about each person, or significant change in existing data-holdings?* b. *New personal data about a significant number of people or a significant change in the population coverage?*	No The types and volumes of data are likely to remain consistent with current levels but the project hopes to make the processing of the data more efficient and effective.

Questions and Guidance Notes	Response
10. *Does the proposal involve new or significantly changed:* *a. consolidation,* *b. inter-linking,* *c. cross-referencing, or* *d. matching of personal data from multiple sources?* *This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.*	Yes One of the primary purposes of the project is to enhance the search capability across the diverse systems and enable a single search to examine all data sources on the platform, subject to the data access rights granted to the individual user.
11. *Does the proposal involve:* *a. New linkage of personal data with data in other collections or* *b. A significant change in data linkages?* *The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called 'front-end verification'), and the matching of personal data from multiple sources.*	Yes The intention is that the enhanced search capability provided when the two systems are co-located on the same platform will enhance the ability to link together records. Although both PNC and PND will be housed on the same platform, it has not yet been determined whether there will be a single data pool or whether the data belonging to each system will be physically or logically separated on the platform. Each system already uses similar identifiers which assist in data matching/linkage.
Data handling	
12. *Does the proposal involve new or changed:* *a. Data collection policies or practices that may be unclear or intrusive?* *b. Quality assurance processes and standards that may be unclear or unsatisfactory?* *c. Security arrangements that may be unclear or unsatisfactory?* *d. Access or disclosure arrangements that may be unclear or permissive?* e. *Data retention arrangements that may be unclear or extensive?*	No
13. *Does the proposal involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?*	No
Exemptions and exceptions	
14. *Does the proposal relate to data processing which is in any way exempt from legislative data protection measures?* *Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.*	Yes The systems concerned process data for law enforcement purposes. In general this will fall within section 29 of DPA 1998 though noting that the s29 exemption only provides an exemption from certain parts of the DPA, to the extent that compliance with those parts will prejudice a

Questions and Guidance Notes	Response
	law enforcement purpose. Processing which is not prejudicial to that purpose is not exempt.
15. *Does the proposal's justification include significant contributions to public security measures?* *Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.*	Yes Improved search and data matching capabilities will enable law enforcement to build up better and more detailed profiles of nominals and organised criminal gangs and thus improve risk assessment in relation to the likelihood of their committing crime, particularly violent crime.
16. *Does the proposal involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable data protection regulation? Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contactors. Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions, such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the UK which are subsidiaries of organisations headquartered outside the UK.*	No
17. *Will the proposal give rise to new or changed data-handling that is in any way exempt from legislative data protection measures?*	No No new data handling involved. See 14 above re exemption from legislative data protection measures.

Annex C – Privacy Law Compliance Check

Does the project involve any activities (including any data handling) that are subject to privacy or related provisions of any statute or other forms of regulation, other than the Data Protection Act?

Yes. The development of LEDS does include data handling activities that are subject to further statutory provisions and regulation, other than the Data Protection Act 1998 (to be replaced when current Data Protection Bill receives Royal Assent.

Consideration of the following acts/regulations will be required in the use and further development of LEDS and the policy/guidance regarding how LEDS, and the data on it, should be used.

1. Human Rights Act 1998

Article 8[8] is particularly relevant to the use of the PND and PNC systems, and to the development of LEDS. The PND links information and intelligence held on local police systems, onto a national system, drawing together information regarding individuals held by one force or other law enforcement agency, which other forces did not previously know existed, creating a wider basis of intelligence. PNC holds detailed information on people including identifying information and, data concerning arrests, charges & court disposals (including convictions); records are also held of those who hold driving licences (or are disqualified from doing so) or firearms licences. All this data will be co-located on the LEDS platform, currently under development, enabling further links to be identified between records.

The retention and processing of police intelligence data and of custody photographs on PND has been challenged under Article 8. The Supreme Court, in the case of R (Catt) v Commissioner of Police of the Metropolis & Anor [2015] UKSC 9, held that the state's systematic collection and storage in retrievable form even of public information about an individual is clearly an interference with private life under the European Convention on Human Rights, art 8(1). Nevertheless the court accepted that retention of data could be justified under Article 8(2). In relation to the uploading of custody images and their use for facial search purposes, the case of R (RMC & FJ) v Commissioner of Metropolitan Police [2012] indicated that the automatic retention of photographs taken on arrest – including where there is no prosecution, or the person is acquitted – for at least six years was an unlawful interference with the right to respect for private life in Article 8. The court decided that the Met's existing policy did not strike a fair balance between the competing public & private interests and did not meet the requirements of proportionality in relation to the retention of photographs of persons arrested but not charged or convicted. Further work is ongoing in this area to address the retention issue.

It is imperative that Article 8 of the HRA is considered at all times during the use of the PND and PNC systems and the development of the LEDS platform; this includes elements of the business regime such as access rights. Currently access rights are restricted dependent

---

[8] **Article 8 Right to respect for private and family life**

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

upon the role of the officer or civilian user, the organisation for which they work and the area of law enforcement in which they operate.

Article 14[9] must also be considered in the context of the information and intelligence that is collated, how it is collected and stored, and how the information is used and shared with others and for what purposes. For example, Article 14 would apply in situations whereby the sharing of information with another country, could lead to an individual being discriminated against due to that country's laws and/or culture.

2. Police Act 1997 – Part V

Part V of the 1997 Act creates a statutory scheme for access by prospective employers to the criminal records and, in limited circumstances, other information held by the police relating to potential employees. It places a duty on Chief Officers of police to provide information, for standard Disclosure and Barring Service (DBS) checks, from 'central records' which refers to conviction and caution information held on the Police National Computer. In the case of enhanced DBS checks, Chief Officers are requested to provide any information in their possession that may be relevant when an employer makes consideration of an applicant's suitability for a position. Such non conviction information is recorded within individual police forces databases and, as such, is placed on the PND. In addition, personal information is redacted for dissemination.

3. The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA), provides the legal basis through which the privacy rights of an individual (created under the Human Rights Act 1998), can be lawfully interfered with. RIPA allows for different levels of intrusiveness, for example the interception of a telephone call which requires ministerial authority, through to looking at telephone records. RIPA also covers varying levels of surveillance, intercepting electronic traffic and communications data.

The nature of some of the data collected by forces requires that there are strict guidelines to forces as to how information and intelligence gathered under RIPA is to be managed, including placing the information onto the PND and how to sanitise it appropriately. Forces are legally obliged to ensure that the data that they enter onto the PND, which has been collected under RIPA, does not conflict with the terms of RIPA. It is necessary that all RIPA information and intelligence be subjected to the 5x5x5 Information/Intelligence Report as outlined under the Guidance on the Management of Police Information, prior to being placed upon the PND. If one force requires further information than that available on the PND, then the appropriate force will need to be contacted.

4. The Investigatory Powers Act 2016

The Investigatory Powers Act 2016 (IPA) provides a legal basis for interference with an individual's right to respect for the privacy of their communications. The IPA regulates how the police (and other agencies) can lawfully acquire communications data, intercept and monitor certain communications equipment as part of a formal criminal investigation or to safeguard the public.

Communications data is information that details who communicated with whom, when and where, but not the content of what was said, written or sent. The IPA allows the Police (and other agencies) to maintain their ability to acquire communications data as new forms of

---

[9] **Article 14 Prohibition of discrimination**

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

communicating have evolved. The IPA also allows the Home Office to require communications companies to retain certain categories of communications data, for longer than ordinary business purposes, where this retention would be in the public interest. Additional consideration should be given to the proportionality of retaining and sharing of this communications data beyond the purpose for which the data was originally obtained.

The content of a communication is given greater protections from privacy interference; the police can only access content of a communication by obtaining an intercept warrant. Police forces can apply for intercept warrants and access the content of communications, but, they can not disclose the content of the intercept material beyond a set of carefully managed individuals. It is unlawful to allow even the existence of an intercept warrant to be known, and data obtained under an intercept warrant can't be disclosed in a UK court of law. To maintain this greater privacy protection the data collected by forces is subject to strict guidelines to forces as to how information and intelligence gathered under IPA is to be managed, including placing the information onto the PND and how to sanitise it appropriately. Forces are legally obliged to ensure that the data that they enter onto the PND, which has been collected under IPA, does not conflict with the terms of IPA. It is necessary that all IPA information and intelligence be subjected to the 5x5x5 Information/Intelligence Report as outlined under the Guidance on the Management of Police Information, prior to being placed upon the PND. If one force requires further information than that available on the PND, then the appropriate force will need to be contacted.

All businesses and organisations, including the police and government departments are permitted under lawful business practice regulations [LBP will come under Investigatory Power Act section 46] to monitor and record communications relating to their business activities. Subject to the LBP regulations and the Data Protection Act information obtained under LBP regulations can be shared with and retained by Police Forces. This includes the content of the communication; however, unlike warranted interception this content can be made public or disclosed if that is appropriate. Therefore different handling arrangements might be appropriate. [E.g. under LBP a 999 call can be made public or disclosed in court].

The IPA permits activities relating to police interference with communications equipment. This equipment interference means interfering with equipment in order to obtain communications, equipment data or other information. The equipment in question could include traditional computers or computer-like devices such as tablets, smart phones, cables, wires and static storage devices. Equipment interference can be carried out either remotely or by physically interacting with the equipment. Additional consideration should be given to the proportionality of retaining and sharing of this communications data beyond the purpose for which the data was originally obtained. Further guidance on the handling of information obtained through equipment interference is contained with the relevant code of practice. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Criminal Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

Further additional protections exist under the IPA for information that relates to certain elected officials (a member of either House of Parliament, the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly, and United Kingdom members of the European Parliament), health professionals, spiritual counsellors (ministers of religion), journalists or journalistic sources and legal advocates, such as solicitors and barristers, where their communications are protected by legal privilege. Police forces must ensure relevant material stored within the PND is protected in line with these additional safeguards.

5. Lawful Business Practice Regulations 2000

The Lawful Business Practice Regulations 2000 are relevant to the information that is stored and accessed upon the PND currently and which will be processed on the LEDS platform

when that data is migrated from PND and PNC. There is potential that intercepted communications information and intelligence will be stored upon the PND. To maintain the integrity of the system, persons inputting the intercepted information should ensure that the material was legally obtained by following the regulations which are summarised below:

The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system.

Interceptions are authorised for:

- *monitoring or recording communications;*
- *to establish the existence of facts, to ascertain compliance with the regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training);*
- *in the interests of national security (in which case only certain specified public officials may make the interception);*
- *to prevent or detect crime;*
- *to investigate or detect unauthorised use of telecommunication systems or,*
- *to secure, or as an inherent part of, effective system operation;*
- *monitoring received communications to determine whether they are business or personal communications;*
- *monitoring communications made to anonymous telephone helplines.*

Interceptions are authorised only if the controller of the telecommunications system on which they are effected has made all reasonable efforts to inform potential users that interceptions may be made.

The Regulations do not authorise interceptions to which the persons making and receiving the communications have consented as these are not prohibited.

Current policing guidelines regarding the use and storage of intercepted material *to prevent and detect crime* must be reviewed to ensure that police forces are compliant with the regulations when using the PND.

6. The Privacy and Electronic Communications Regulations 2003

These Regulations are concerned with the regulating of direct and indirect marketing through electronic means. This are not relevant to PND, PNC or to the LEDS platform as none of the systems are, or will be, involved in any such marketing, neither will they send out e-mails to individuals to gather support for charitable organisations and/or political parties.

7. Common Law of Confidentiality

Traditionally, the English common law has protected an individual's right to expect that personal information about him or her will be kept confidential. Information will be protected if it has "the necessary quality of confidence about it" and has been provided or obtained in circumstances imparting an obligation of confidence. For example, information given to a doctor, social worker or lawyer would normally be considered to have this quality of confidence, but a conversation with a friend would not. A duty of confidentiality may also arise as a result of a contract where one party agrees to keep confidential information provided by the other party.

A court can prevent the disclosure of confidential information by injunction and, where appropriate, award damages if unlawful disclosure has been made.

The law imposes a 'duty of confidence' whenever a person receives information they know or ought to know is fairly and reasonably regarded as confidential. The confidentiality can either be **implicit** or **explicit:**

Implicit – Where the nature of the information and circumstances imply that a person should keep the information confidential, there is **an implied duty of confidence**. In particular, where disclosure of that information could cause substantial harm or offence, or it is self-evidently confidential, or implicitly confidential by custom and practice e.g. relationship between employee and employer or client and solicitor or doctor and patient.

There will often be an implicit duty of confidence where a public authority has statutory powers to obtain information.

Explicit – There is a duty of confidentiality where a person or organisation **expressly agrees** to keep information confidential, provided the information has the necessary **quality of confidence** e.g. confidentiality clauses in contracts and agreements.

There are two main exceptions to the duty of confidence. Firstly, public interest can override the duty. For example, a psychiatrist could pass on information about a patient to the police if it was felt that the patient was a danger to third parties. Secondly, disclosure of confidential information may be permitted or required by statute or court order.

Information and intelligence gathered prior to, and following the implementation of the PND, could be subject to the common law of confidentiality; information on PNC may also be subject to this common law duty. Policy should be considered as to how, if necessary, the information imparted to an officer can be used, and how an individual is informed (at point of original contact, or prior to the use of the information) about how their information will be processed.

8. Tort of Privacy

Although there is no legal tort of privacy in the United Kingdom, there is evidence to suggest that it is emerging in case law. With regard to this, the NLEDP should look at recent cases in which privacy is cited to understand what future provisions may need to be built into the system and be mindful of case law concerning the retention of personal information, images, prints and other biometric data which is likely to develop further such as the recent cases brought under the Human Rights Act.[10] There is an expectation on forces to comply with these cases in this area.

Tort law is a branch of civil law, and is defined as a legal wrong. In civil law the dispute is typically between private parties. However, governments can also be sued. An action in tort is defined by Her Majesty's Court Service as *'a claim for damages to compensate the claimant for harm suffered. Such claims arise from cases of personal injury, breach of contract and damage to personal reputation. As well as damages, remedies include an injunction to prevent harm occurring again.'*

9. The sharing of information on children and young people

The sharing of information on the PND and PNC (and subsequently on LEDS) must give regard to the guidance (*Information Sharing: Practitioners' guide)*, and advice that the Department for Children, Schools and Families (DCSF) provides for the sharing of information relating to children and young people.

---

[10] R (RMC & FJ) v Commissioner of Metropolitan Police (2012) R (Catt) v the Commissioner of Metropolitan Police (March 2015) Gaughran v Chief Constable of the Police Service of Northern Ireland (13th May 2015) S and Marper v UK (2008)

The Guidance provided by DCSF, as part of the Every Child Matters scheme, is non-statutory guidance; however, it provides strong advice as to how and when personal information regarding children and young people can and should be shared.

Police personnel should regard the guidance when processing information about children and young people, and when sharing that information. In particular, care must be taken when information or intelligence is placed on the PND, potentially becoming accessible to Child Protection Unit officers on a national scale. The migration of PND data to LEDS and the potentially larger number of user organisations outside the Police Service which will have access to the new platform requires that adequate security measures be designed and put in place to restrict access to this data on a "need to know" basis to avoid accidental access to or disclosure of such information.

The DCSF Guidance recommends that consent is sought for the sharing of information either from the child/young person if they comprehend and are able to make a sound decision, or from a responsible adult. Information concerning the child/young person can be shared without consent if it is believed to be in the public interest that the information is shared, or that the child/young person 'may be suffering or may be at risk of suffering serious harm.'

Information sharing may also be necessary if there is a statutory purpose to share the information, or if the information is the subject of a court order.

10. Police and Criminal Evidence Act (PACE) 1984

This legislation is particularly relevant to the information collected and processed on PNC in relation to arrests, charges, prosecutions, convictions and cautions; due regard is also given to PACE in relation to the retention and storage of information and intelligence on the PND system, and the manner in which that data is utilised by authorised users of the PND. Going forward, PACE requires consideration in relation to the development and implementation of the LEDS platform.

The PACE Codes of Practice are outlined below.

- PACE Code A – deals with the exercise by police officers of statutory powers to search a person or a vehicle without first making an arrest. It also deals with the need for a police officer to make a record of such a stop or encounter.
- PACE Code B – deals with police powers to search premises and to seize and retain property found on premises and persons.
- PACE Code C – sets out the requirements for the detention, treatment and questioning of people in police custody by police officers.
- PACE Code D – concerns the main methods used by the police to identify people in connection with the investigation of offences and the keeping of accurate and reliable criminal records.
- PACE Code E – deals with the tape recording of interviews with suspects in the police station.
- PACE Code F – deals with the visual recording with sound of interviews with suspects.
- PACE Code G – deals with statutory powers of arrest; and
- PACE Code H – deals with the detention of terrorism suspects.

Section 64A of PACE provides the authority to photograph arrested persons in Custody units and the facial search functionality added to PND compares these photographs against facial images obtained from other sources.

PACE forms an integral part of understanding how the PND and PNC are used currently and how they can be used on the new platform once developed as PACE forms the legislative framework for policing powers.

11. Criminal Procedures and Investigations Act 1996

Further work is required as to how the type of information and intelligence on the PND (again including audit logs) is collated and stored to ensure that *the information which is obtained in the course of a criminal investigation and may be relevant to the investigation* is correctly retained for the purposes of the Criminal Procedures and Investigations Act 1996. A failure to ensure this is managed correctly for the PND could result in errors occurring at a later stage in the criminal justice system.

12. Computer Misuse Act 1990

The Computer Misuse Act covers three offences:

- unauthorised access to computer material (for example out of curiosity);
- unauthorised access with intent to facilitate the commission of a crime (for example fraud or blackmail); and
- unauthorised modification of computer material (for example fraud or blackmail).

The Computer Misuse Act relates in two main ways to the implementation of the PND and PNC and to the development of LEDS, particularly the information and intelligence that is held, or made accessible, via the systems.

Primarily PND & PNC must continue to be secure systems that strongly inhibit and deter misuse of the system both by authorised users or external threats. Both systems have audit functionality whilst PND also has system alerts, both of which are likely to identify breaches of security. These security considerations will be included in the design and development process for LEDS. Individuals or agencies which are caught breaching or attempting to breach security are dealt with under internal disciplinary procedures, the Computer Misuse Act, the Data Protection Act (data theft or disclosure) or the common law offence of misconduct in a public office as appropriate.

Secondly, authorised users of the PND and PNC systems need to understand the security access level that they have been granted and the reasons behind that decision. It is strongly recommended that users are reminded of the Computer Misuse Act and that improper use of either system could result in disciplinary procedures or prosecution. All user activities on PND and PNC are auditable and this effective audit regime will be designed for the LEDS platform.

13. Official Secrets Act 1989 (OSA) & The Official Secrets Act 1989 (Prescription) (Amendment) Order 2012

Individuals with authorised access to the PND will need to be made fully aware of their duties under the Official Secrets Act 1989.

Individuals working with sensitive information are commonly required to sign a statement to the effect that they agree to abide by the restrictions of the OSA. Whether this is the case or not, they are bound by the OSA's requirements.

It should be noted that the Act applies in England, Wales, Scotland, Northern Ireland, the Isle of Man and the Channel Islands.

14. Management of Police Information (MoPI) Code of Practice and Guidance

The MoPI Code of Practice and Guidance form a package to which Chief Officers must have 'due regard' under the terms of the Police Act 1996. The development and ongoing functionality of the PND takes into consideration the management of police information and intelligence as required by MoPI. Particular importance is given to the following five business areas:

- Intelligence;
- Crime;
- Custody;
- Child Abuse and
- Domestic Violence

The Code and Guidance set out a framework for the management of police information based on the principle that effective policing is dependent on efficient information management. It is essential that a policing purpose is established in order for information to be legally held. All aspects of the Code and the Guidance are incorporated into the work towards the ongoing development and implementation of the PND.

Annex D – Consultation

For this initial iteration of the LEDS PIA, carried out during the early phase of the Programme, consultation was carried out with the following stakeholders: -

NLEDP team members (including project leads, data and security architects, business analysts and business process leads).

Home Office Biometrics

Police National Computer subject matter specialists

Police National Database subject matter specialists

External consultation was conducted with the Information Commissioner's Office

It is intended that future reviews of this PIA will include consultation with the police service, the wider community of user organisations and with the public.