Data Protection Impact Assessment

Law Enforcement Data Service (LEDS)

V3.0

Contents

Preamble 3
Purpose 3
Step 1: Introduction 4
Step 2: Describe the processing 7
  Processing Operations 7
  Nature of the Personal Data 19
  Data Subjects 24
Step 3: Consultation 27
Steps 4 & 5: Identify risks, assess risks, and determine measures to reduce risks 28
Annex A: LEDS DPIA Glossary 41

Preamble

The LEDS Joint Controllers (the police forces of England, Wales, Scotland and Northern Ireland and the National Crime Agency) are required to comply with Data Protection legislation – (i) the Data Protection Act 2018 (DPA) when they process personal data for any of the Law Enforcement Purposes, and (ii) the UK GDPR, as supplemented by the DPA, when the processing is for General Purposes (anything that does not fall under the Law Enforcement Purposes definition).

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

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

The DPIA must be undertaken prior to the processing starting and, in some cases, cannot commence without the prior authorisation from the Information Commissioner's Office (ICO)[1] once they have reviewed the DPIA.

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

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

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

Purpose

This DPIA document has been used to:

- identify any privacy or information risks concerning the processing of personal data.
- determine any mitigations necessary to bring those risks down to an acceptable level.
- provide a record of those mitigations.

[1] The Data (Use and Access) Act 2025 will abolish the Information Commissioner's Office, in place of which will be a newly empowered Information Commission with an expanded regulatory and enforcement remit.

Step 1: Introduction

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

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

The Law Enforcement Data Service (LEDS) is being developed to modernise and replace the Police National Computer (PNC), which was established in 1974 and is nearing the end of its service life. LEDS will provide a modern platform to support policing and law enforcement activity across the UK.

LEDS enables authorised police forces and other Law Enforcement Agencies to access and update national policing records. These records include information about people, vehicles and property where this is relevant to policing and public safety functions.

LEDS also supports access, where appropriate, to information held by partner organisations, including motor insurance data held by the Motor Insurers' Bureau (MIB), driver and vehicle records held by the Driver and Vehicle Licensing Agency (DVLA), and vehicle test records held by the Driver and Vehicle Standards Agency (DVSA).

LEDS is certified to British Standard BS 10008, which sets standards for the integrity and evidential value of electronic information. The technical development of LEDS is managed by the Home Office on behalf of the LEDS Joint Controllers, in line with agreed contractual arrangements.

LEDS is used to create and maintain national records in support of law enforcement functions, including records relating to arrests, charges and convictions, people wanted by law enforcement, and missing persons.

Where appropriate and lawful, information may be shared with other law enforcement bodies and relevant third parties in support of policing purposes, supported by governance and data-sharing arrangements.

In addition to UK-based organisations, LEDS is used by Law Enforcement Agencies in the Crown Dependencies (the Bailiwick of Jersey, the Bailiwick of Guernsey and the Isle of Man). If access is provided to Gibraltar-based Law Enforcement Agencies in future, an appropriate international transfer mechanism would be identified.

LEDS supports the processing of criminal convictions and other court outcomes for England and Wales. Scotland and Northern Ireland maintain separate conviction registers for their jurisdictions. LEDS may also hold conviction information shared with the LEDS Joint Controllers by non-UK authorities, where this is lawful and relevant.

LEDS is comprised of a set of 'Services', each of which provides functionality to users in accordance with their access level entitlements. These Services include:

- Person
- Drivers
- Vehicles

- Property
- Audit
- Broadcast
- Interest Search
- Data Compliance Logging Service (which is superseding the Disclosure Logging Service).

The personal data in LEDS is processed for law enforcement, policing, and wider public safety purposes including National Security.

All Services in LEDS will be operational in 2026 whilst continuing to evolve. To enable organisations to safely transition from the PNC to LEDS, there will be a period of dual running of the two systems, with data being replicated on each, until the PNC is decommissioned.

This DPIA will be periodically updated to reflect the evolving nature of the Service.

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

LEDS arose from the requirement to have a replacement processing service to succeed the PNC which is approaching end of service life.

The development of LEDS is supported by the Policing Vision 2025 which set a clear agenda for why and how the police service needs to be transformed. It specifically called out the need for Policing to adapt to the modern policing environments, such as dealing with 'high harm' crimes by utilising more modern IT systems. The Vision identifies that the 'increasing availability of information and new technologies offers us huge potential to improve how we protect the public'. This ambition is reiterated in the Policing Vision 2030, and LEDS specifically supports Pillar 2 (to prevent crime and criminality) and Pillar 3 (to respond effectively to all appropriate demand and bring perpetrators to justice).

In addition, other influences on the need for change centre on the diminishing pool of resource with knowledge of the PNC (which is now over 50 years old) and limitations relating to hardware and software making it increasingly difficult to support.

Only a new modern service, such as LEDS, can deliver what Policing and Law Enforcement users need today and allow it to adapt to future needs.

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

LEDS is primarily used to process data for Law Enforcement Purposes. These are defined in Part 3 of the Data Protection Act 2018 (DPA).

Other processing in LEDS is undertaken for General Purposes under the UK General Data Protection Regulation (GDPR) and Part 2 of the DPA. This processing includes, but is not limited to:

- National security vetting
- Safeguarding children and vulnerable people

- Missing people
- Health & safety (of staff, officers and the general public)

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

There are several legal and regulatory frameworks guiding the use of such data. These include, but are not limited to:

- Health & safety
- Common Law duties/powers
- The National Police Records (Recordable Offences) Regulations 2000 (S.I. 2000/1139)
- The Police and Criminal Evidence Act 1984 (recordable offences)
- The Criminal Justice and Public Order Act 1994
- The Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002
- The Police Act 1996
- The Offender Management Act 2007
- The Criminal Justice Act 1991
- The Criminal Justice Act 2003
- The Crime and Disorder Act 1998
- The Police Information and Records Management: Code of Practice 2023
- The Regulation of Investigatory Powers Act 2000
- The European Convention on Human Rights Act 1998
- The PNC and LEDS Code of Practice 2023
- The Police & Fire Reform (Scotland) Act 2012 (sections 20 & 32)
- The Children's Act 1989
- The Mental Health Act 1983
- UK Borders Act 2007
- Immigration Act 2016

Step 2: Describe the Processing

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

Processing Operations

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

LEDS draws together data from local and national policing systems, providing an inherent set of data, for which the Police and Law Enforcement are responsible. Data is also available via interfaces from other organisations, supporting Law Enforcement activities.

Data is obtained/created from several sources including:

- The person whose data is being processed (Data Subject)
- An associate of the Data Subject
- Police and other Law Enforcement Agencies
- Commercial organisations
- Other public authorities

Data in LEDS is made available via:

- Direct entry by LEDS users creating a new, or updating an existing record
- Access to data held by third-party organisations via Application Programming Interfaces (APIs)
- Interfaces to local Policing systems and other national Law Enforcement systems

When:

LEDS data is available to authorised direct and interface users at all times, year-round. Data extracts are also shared with Policing, Law Enforcement and third-party organisations on an agreed periodical basis via Managed File Transfer (MFT) or via Email/Notifications.

Personal data is processed through the following services:

- Person
- Drivers
- Vehicles
- Property
- Audit
- Broadcast
- Interest Search
- Data Compliance Logging

Privacy Notices informing Data Subjects how their information is processed within LEDS are maintained and published by individual Controllers as part of their legal responsibilities.

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

The processing of personal data varies depending on the data set involved.

All authenticated users can access the data needed to fulfil their operational needs, using password protected and authorised devices, as per the entitlements assigned to their role by a local administrator.

The data in LEDS may be shared on an ad-hoc basis, upon request, for safeguarding purposes.

The details of the LEDS data sets (or Services):

1. Person Service

The Person Service holds individuals' data within LEDS. It allows users with the appropriate entitlements to search for, view and update national records. There are an estimated 39 integrations, including interfaces and data extracts, that will migrate from the Police National Computer (PNC) prior to its decommissioning. External systems are managed by organisations outside of LEDS and may consume data from LEDS, provide data to LEDS, or do both. This includes other Home Office departments. Users have direct access via the user interface, which may also be available on police-issued mobile devices, such as tablets and mobile phones.

Processing operations will occur 24 hours a day, 7 days a week and can be broken down to include, but not limited to:

- Collection – personal data is obtained directly from Data Subjects or their associates, and input by Law Enforcement officers and staff. Data can also be obtained from various other technical and non-technical sources, such as through data sharing with third-party organisations.
- Use – the data is used primarily for Law Enforcement, Policing, and public safety. In some cases, processing occurs as part of safeguarding responsibilities under UK GDPR. Additionally, other non-policing users may also use the data, determined by the LEDS Joint Controllers.
- Storage – the data is stored in a secure cloud hosting service within the UK.
- Amendment – the Law Enforcement organisation that initially entered the data can make changes to add to, or correct, the data which will be captured on LEDS.
- Search – this functionality matches users' searches with records on LEDS. Records can also be linked by biometric (DNA & fingerprints) references, linking records to the national fingerprint identification system (IDENT1) and the National DNA Database (NDNAD). Searches are based on 'NASCH' or unique references such as a 'PNCID'. No actual biometric data is stored within LEDS Person Service.
- Sharing – LEDS Person data is shared using several secure means, including via APIs and the Web application user interface (for direct LEDS users). Data is also shared with authorised organisations and is managed using Data Sharing Agreements, Memorandums of Understanding and Data Processing Agreements. Any disclosure of data outside of LEDS will comply with the logging

requirements under Section 62 of the DPA, capturing the date/time of disclosure and to whom the data has been disclosed. The justification for disclosure is also logged.

- Export – Export to Clipboard is a method for extracting and sharing information from LEDS Persons. This functionality facilitates the operational need for Control Room staff to extract data from LEDS Persons and provide it directly to frontline officers via local force systems, accessible through mobile applications.
- Erasure – records are maintained according to the PNC retention schedules and in line with the principles of the Code of Practice on police information and records management. This will remain in place until NPCC's Retention, Redaction and Deletion schedule has been completed and implemented.
- Restrictions – access to Person data will be restricted to authorised users/organisations and managed via the use of entitlements. Restrictions on the use of that data will be defined in Data Sharing Agreements where sharing takes place.

2. Drivers Service

The Drivers Service facilitates checks against driving licence information held by the Driver and Vehicle Licensing Agency (DVLA) and enables Road Policing Officers and other investigators of road traffic matters to establish a person's identity, current Driving Licence status, entitlement to drive and other restrictions.

The Crime and Policing Act 2026 introduces Section 71A in the Criminal Justice and Court Services Act 2000, allowing authorised persons to access driver licence information held by the DVLA for any Policing or Law Enforcement Purpose – not just road traffic offences[2].

LEDS Drivers also provides driver-validation capabilities, formerly delivered by the DVLA Driver Validation Service (DVS), including confirmation of driver identity, licence status, and driving entitlements for lawful law enforcement purposes.

- Collection – driving licence data is accessed from the DVLA data set via an API.
- Use – the data is available to use by Policing and Law Enforcement for the purpose of prevention, investigation or prosecution of a contravention relating to road traffic matters as supported by the relevant legislation. Once the provisions of the Crime and Policing Act are implemented, the data will be available to use for any Policing or Law Enforcement Purpose.
- Storage – DVLA data is not stored in LEDS Drivers as the data is processed via an API Service. When an enquiry is made on a Driver record, data is available for 15 minutes in the cache and then cleared. However, the data from DVLA may be manually added to police records which are stored in other LEDS Services e.g. Vehicles & Person Services.
- Amendment – data accessed via the API is read-only. DVLA data cannot be altered, merged, or changed by LEDS users.
- Search – if a user search matches records within the DVLA dataset, the Service will only return the first 50 records for a basic driver search, with a total of 10 items per page. For enhanced searches, the Service will return the first 200 records. Thumbnail images will be provided if available, which the authorised

[2] This will come into effect once statutory regulations and a Code of Practice are in place.

Police or Law Enforcement user will need to select on screen before requesting the search.

- Sharing – data is shared with approved third-party organisations to support Law Enforcement activities, in accordance with Memorandums of Understanding (MOU) and Data Sharing Agreements. Any disclosure of data outside of LEDS will comply with the logging requirements under Section 62 of the DPA, capturing the date/time of disclosure and to whom the data has been disclosed. The justification for disclosure is also logged.
- Export – Export to Clipboard is a method for extracting and sharing information from LEDS Drivers. This functionality facilitates the operational need for Control Room staff to extract data from LEDS Drivers and provide it directly to frontline officers via local force systems, accessible through mobile applications.
- Erasure – data accessed via the API is read-only. DVLA data cannot be erased by LEDS users.
  Restrictions – access to driving licence data is restricted to authorised persons and managed via the use of entitlements. Use of the data is restricted to the permitted purposes agreed in the MOU between the DVLA and LEDS Joint Controllers.

Note: The Photos at the Roadside Service (PARS) is provided by DVLA and enables Police and Law Enforcement to access a driver's facial image following a search for their information on PNC. PARS has been in use by several forces and will be phased out and incorporated into the LEDS Driver Enquiry API.

3. Vehicles Service

The Vehicles Service facilitates checks against the Vehicle Registration Mark (VRM) or the Vehicle identification Number (VIN). LEDS provides API services that access Driver and Vehicle Licensing Agency (DVLA) data regarding the vehicle itself (e.g. make, colour, registered keeper, whether the vehicle is taxed), Motor Insurers' Bureau (MIB) data on the vehicle's insurance status and Driver and Vehicle Standards Agency (DVSA) data on whether the vehicle has a valid MOT test certificate. Enquiries via the Vehicles Service currently averages about 4,300,000 transactions per month (52,000,000 per year) and this is expected to be the same for the API service.

- Collection – Vehicle data is collected by authorised users from the roadside, or from other third-party organisations such as DVLA, DVSA and MIB.
- Use – the processing may be for a Law Enforcement Purpose, as Police and Law Enforcement carry out their functions under Schedule 7 of the DPA as a competent authority. It may also be used for General Purposes and as defined in agreement between the parties, e.g. MIB data.
- Storage – the Service facilitates the storage of police reports relating to Vehicles of Interest only.
- Amendment – initially, LEDS will be reliant on PNC for police reports and markers, such as those placed on stolen and recovered vehicles. This data is shared with the DVLA for them to update their dataset. LEDS users cannot update or amend DVLA data. If there is a discrepancy noted by a force when they view data from DVLA, they must inform the DVLA in writing.
- Search – LEDS will display basic VRM details along with all police markers. When a Vehicle Search is made, the Service may request information from

external databases such as the DVLA, DVSA, MIB and (in the interim) PNC. This is shared with users based on their entitlements, within headed tabs to minimise its availability.

- Sharing – data is shared with approved third-party organisations to support Law Enforcement activities, in accordance with Memorandums of Understanding (MOU) and Data Sharing Agreements. Any disclosure of data outside of LEDS will comply with the logging requirements under Section 62 of the DPA, capturing the date/time of disclosure and to whom the data has been disclosed. The justification for disclosure is also logged.
- Export – Export to Clipboard is a method for extracting and sharing information from LEDS Vehicles. This functionality facilitates the operational need for Control Room staff to extract data from LEDS Vehicles and provide it directly to frontline officers via local force systems, accessible through mobile applications.
- Erasure – records are maintained by the LEDS Joint Controllers according to the PNC retention schedules. Other controllers will process Vehicle data based on their own retention and deletion policy.
- Restrictions – access to vehicle data is restricted to authorised users/organisations and managed via the use of entitlements. Use of the data is restricted to the permitted purpose/s defined in MOUs between the LEDS Joint Controllers and the DVLA, the DVSA and the MIB.

4. Property Service

The Property Service represents the national stolen and found property register. This is the first service which makes property data fully available to both policing and Law Enforcement. Property data is also made available via extracts to authorised non-police organisations.

- Collection – data is collected from those that have lost or had items stolen, as well as those that have subsequently found items and have chosen to record this with the Police (directly or indirectly).
- Use – this Service provides Police and Law Enforcement with access to nationally circulated stolen and found property records, to solve crime and return property to its rightful owner. Users can view individual property details in (PDF) and view property history.
- Storage – the data is stored on LEDS and available to users as part of a structured and referenced data set available on the user interface.
- Amendment – LEDS users need to have the edit function to make amendments to property items. However, this functionality is only available to authorised users within the 'owning force' for that property item; or an alliance/collaboration force – where such agreements are in place.
- Search – via alphanumeric identifier, descriptive terms, elastic search implemented behind alphanumeric identifiers. Global search allows users to search with keywords, date and owning force. The aim is to record items of high value/ significance, where circulating information at a national level will better support Policing.
- Sharing – data is shared with third-party organisations in accordance with Data Sharing Agreements. Any disclosure of data outside of LEDS will comply with the logging requirements under Section 62 of the DPA, capturing the date/time of disclosure and to whom the data has been disclosed. The justification for disclosure is also logged.

- Export – Export to Clipboard is a method for extracting and sharing information from LEDS Property. This functionality facilitates the operational need for Control Room staff to extract data from LEDS Property and provide it directly to frontline officers via local force systems, accessible through mobile applications.
- Erasure – the retention period for property data is determined by its type and status. For stolen items like plants, engines, trailers or animals, the retention period is six years, while for firearms, marine and aircraft items it is ten years. Found items have a one-year retention period. Items previously marked as stolen have a six-week retention period. Local reviews can extend the retention period by one year if necessary. Data will be automatically weeded on its weed date unless manually deleted earlier. Notifications are sent six weeks before the weed date to prompt reviews.
- Restrictions – access to vehicle data is restricted to authorised users/organisations and managed via the use of entitlements. Restrictions on the use of that data are defined in Data Sharing Agreements where sharing takes place.

5. Audit Service

The LEDS Audit Service captures, stores, and provides access to end-to-end records of the activities undertaken on LEDS, including personnel data related to the users – such as Officer's Collar Number or a user's name. It also captures and stores data relating to automated (non-user initiated) activities. This supports organisational Auditors to identify misuse, whether this is malicious or otherwise. The Audit Service enables enquiries to be carried out as part of investigations into misconduct or other legal proceedings. The Audit Service also utilises tools with the ability to conduct 'audit the auditor' checks.

- Collection – Section 62 of the DPA requires that the processing of data on LEDS should be recorded, stored and logs provided of users' interactions with the Service. Whilst the legislative requirement to collect audit data only applies to Law Enforcement Processing, the Service captures all LEDS user activity, regardless of which regime the processing relates to.
- Use – the Audit Service is used to provide chronological details of the creation, updating, amending, erasure or sharing of any record on LEDS for logging and investigative purposes. Auditors have four different levels of data access, designed to meet the specific needs of differing users. Data processed by Audit will also be related to users of LEDS (including Police Officers, Police Staff and non-policing users). The LEDS National Auditor has oversight of all Joint Controllers' audit records.
- Storage – data is stored in LEDS and kept for seven years.
- Amendment – Auditors do not have entitlements to apply updates or amendments to any LEDS data whilst being an Auditor.
- Search – the Audit Service divides user data into three categories, depending on the level of data required. It enables an Auditor to manage the amount and level of data returned upon an audit search. The Auditor is not presented with a large amount of data to assess. If additional information is required, then this can be requested by the Auditor progressively.
- Sharing – The Audit logs are shared with Local Auditors and contain data relating to their organisation. The Service also shares log details with a National Auditor who oversees the activities of Local Auditors. Data from the logs may be

shared with Professional Standards and Anti-Corruption Units to provide evidentially sound audit trails for the purpose of facilitating misconduct or legal proceedings.

- Erasure – after seven years, LEDS will flag a proposal to delete. This will be automatically applied unless there is an override to keep the data stored, e.g. for an ongoing prosecution. Audit data is immutable and cannot be deleted through user action.
- Restrictions – the Audit Service is restricted and is only available to specified and limited numbers of organisational level Auditors. They are overseen by a National Auditor. It is their responsibility to ensure that force Auditors are accessing and utilising their responsibilities appropriately. Auditors do not have entitlements to update any part of LEDS whilst being an Auditor.

6. Broadcast Service

The Broadcast Service is used by Police forces and other Law Enforcement Agencies to send routine, urgent and critical messages to each other, individually or in groups of organisations depending on the requirements of the message.

- Collection – data used to create a Broadcast message is collected from other LEDS Services (Person, Vehicles, Property) or from other sources outside of LEDS including the Data Subject, an associate of the Data Subject, Law Enforcement agencies or other government departments.
- Use – data is used within the Broadcast Service for the purpose of relaying routine, urgent and critical messages to support operational policing.
- Storage – when Broadcast messages are created, they are dispatched into the LEDS SMTP Notifications Service and stored for seven days, after which time they will no longer be available to view by the recipient.
- Amendment – Broadcast messages cannot be amended or withdrawn once they have been created and sent, however subsequent messages can be sent to provide further information or correct any inaccuracies in a previous broadcast. The message is read-only for recipients.
- Search – users can search for a Broadcast message using the Broadcast ID number.
- Sharing – Broadcast messages are shared with Police forces and other Law Enforcement Agencies, individually or in groups of organisations depending on the requirements of the message. Any disclosure of data outside of LEDS will comply with the logging requirements under Section 62 of the DPA, capturing the date/time of disclosure and to whom the data has been disclosed. The justification for disclosure is also logged.
- Erasure – Broadcast messages, once created and sent, cannot be recalled or erased. After seven days, the messages are subject to automatic deletion. The erasure activities are logged by the Data Compliance Logging Service. All user interactions with the LEDS Broadcast application are logged by the LEDS Audit Service. All logs are automatically deleted after a period of seven years.
- Restrictions – Broadcast messages will only be sent to pre-configured recipients lists and approved email domains that have undertaken rigorous security assurance processes. Access to this Service will be available via entitlements to a restricted userbase.

7. Interest Search Service

The Interest Search Service allows users to search on other search events within LEDS. It supports a proportion of the audit functionality in PNC known as Transaction Enquiry (#TE) and is designed to be used by Officers as part of their investigative activities. This Service is separate from the Audit Service used by compliance Auditors, Professional Standards Departments, or any other investigation into the legitimate use of policing data.

- Collection – this Service captures logs of what LEDS users have been searching for across a suite of other LEDS Services.
- Use – users can search on other search events within LEDS. Search parameters available to a user are based on their type of entitlement. The records which are returned will be used by Policing and Law Enforcement to support their investigative activities.
- Storage – Interest Search data is stored for a period of seven years and is then subject to automatic deletion.
- Amendment – Interest Search data is immutable and cannot be adapted through user action.
- Search – users can search on criteria and establish if another user has searched for those criteria. Users have access to 'Activity' level data from Vehicles, Person, Property, Drivers and Interest Search Services.
- Sharing – an application programme interface (API) is in use to allow LEDS Services to communicate with each other and with external parties such as DVLA.
- Erasure – Interest Search data is immutable and cannot be deleted through user action.
- Restrictions – the Interest Search Service captures and presents read-only data relating to 'Activity' level (level 2) details. Users cannot create, edit or delete a record, nor can they see if a record has been viewed, that a record exists, or the personal data viewed by any LEDS user, some of which may be sensitive. Users cannot see any underlying Policing data associated with a LEDS/PNC record.

8. Data Compliance Logging Service[3]

The Data Compliance Logging Service (DCLS) is responsible for capturing and storing logs of processing activities that are occurring across the other LEDS Services (Person, Drivers, Vehicles, Property, Broadcast, etc) including collection, alteration, disclosure, combination and erasure of data.

- Collection – data is collected by logging processing activities that are occurring across other LEDS Services.
- Use – disclosure logs may be used for investigative or compliance monitoring purposes.
- Storage – records are stored securely within this Service using AWS infrastructure, in the event those records need to be reviewed for investigative or compliance monitoring purposes. After a period of seven years those records are subject to automatic deletion.
- Amendment – this is a logging service and therefore data cannot be adapted.

[3] The Data Compliance Logging Service is superseding the Disclosure Logging Service which captures and stores logs of disclosures only.

- Search – activity logs can be searched for and made available on request.
- Sharing – if data logs need to be reviewed for investigative or compliance monitoring purposes, the DCLS can make data available upon request.
- Erasure – data logs captured and stored by this Service cannot be manually erased.
- Restrictions – data compliance logging is restricted to capturing and storing relevant processing activities that are occurring across other LEDS Services.

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

The main bodies processing data will be Policing and Law Enforcement, under a Joint Controllership Agreement (JCA) which is in place between the 43 geographical police forces of England and Wales, British Transport Police, Civil Nuclear Constabulary, Ministry of Defence Police, Police Service of Scotland and Police Service of Northern Ireland, along with the National Crime Agency.

Any data entered onto LEDS by any of the Joint Controllers will become the subject of the joint controllership.

The Ministry of Justice (MoJ) has confirmed a continued operational requirement to access court conviction data to support statutory justice functions. To mitigate risks relating to controller accountability and purpose limitation, the MoJ will undertake a data protection/assurance assessment to review the processing of this data within LEDS, with existing access arrangements maintained to ensure continuity and any outcomes reflected through an updated DPIA and associated governance documentation.

Other Law Enforcement Agencies (LEAs) and non-LEA organisations (non-LEAs) may also be given access by the LEDS Joint Controllers, to components of LEDS to enable them to fulfil their functions. Data Sharing Agreements are in place to define the processing with these organisations on a Joint Controller-to-Controller basis.

In addition to third-party organisations being given access to LEDS data, other third-party organisations may be Controllers of data being processed on LEDS with the objective of sharing data with the LEDS Joint Controllers.

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

The LEDS Joint Controllers have appointed the Home Office as a Processor to provide the IT infrastructure. The Home Office has appointed Amazon Web Services UK Branch as a sub-processor to provide the cloud-hosting services.

A Data Processing Contract for LEDS is in place between the Joint Controllers and the Home Office as a processor. A sub-processing contract is in place between the Home Office and Amazon Web Services.

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

The use of national policing systems, such as LEDS, in democratic societies is common and largely expected by individuals and civil society groups. Maintaining a

single point of truth, through such databases, makes it easier for organisations and institutions with appropriate access to carry out their responsibilities. Members of the public would expect personal, sensitive data to have the strongest protection against inappropriate access to that data. As a modern service, LEDS will be utilising technical and organisational tools to ensure the data is protected. These will be adaptable to meet the changing nature of Law Enforcement.

There is information in the public domain which relates to LEDS as a replacement for the PNC. In February 2023, the PNC and LEDS Code of Practice passed through UK Parliament. This was after a period of public consultation on it during the previous year.

To reduce the likelihood of any issues arising related to the processing, particularly to vulnerable members of the public, the following activities have been undertaken:

- An Equality Impact Assessment (EIA), as required under the Equality Act 2010 via the Public Sector Equality Duty (PSED). This seeks to ensure that public bodies play their part in tackling discrimination and inequality and contribute to making society fairer. It reduces the likelihood of any discriminative or adverse impacts on groups with protected characteristics[4], which may be caused by their data being processed in LEDS. The assessment will continue to monitor and advise the LEDS Product Teams to ensure any decisions are taken with an understanding of potential and unintended impacts on individuals with protected characteristics.
- A Child Rights Impact Assessment (CRIA) has been undertaken to help identify any LEDS development plans that might mitigate the negative impacts on children's rights and maximise the positive impacts for children. It is intended to demonstrate compliance with the United Nations (UN) Convention on the Rights of the Child and is deemed good practice.

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

The volume of personal and sensitive data held within, and shared outside of, LEDS has the potential to pose a risk to the confidentiality of that data. Such processing may engage Article 8 of the European Convention on Human Rights (ECHR), as it involves interference with an individual's right to respect for private life. However, Article 8 rights are qualified and may be lawfully interfered with where the processing is necessary and proportionate for a legitimate aim.

Risks to the confidentiality of individuals' personal data are mitigated through the application of appropriate technical and organisational measures within LEDS. Following the implementation of these measures, no high residual risks have been identified.

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

The use of public cloud-based providers as a means of sharing data, alongside APIs, has become commonplace across many sectors including local and central government in the UK. Within policing and law enforcement, this approach

[4] The Equality Act 2010 defines nine characteristics that are protected from discrimination.

continues to be supported through established and assured platforms and networks.

The processing largely resembles that which has been undertaken by Policing and Law Enforcement for many years using the PNC, which is being replaced with LEDS to utilise modern technology and reduce physical data storage.

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

There are numerous measures used to protect the data which include technical solutions and organisational mitigations to reduce the risk to the confidentiality of the personal data being processed. These include:

Organisational:

- The Police Digital Service (PDS) is the key body that supports policing to deliver its digital strategy and assist with oversight of information assurance.
- The statutory PNC and LEDS Code of Practice sets out the need for robust arrangements to be in place to ensure appropriate security of the data, including protection against unauthorised access.
- The Police Information Access Panel (PIAP) considers applications for access to LEDS, including any requests for downloads and data extracts. PIAP also considers requests for organisations which access LEDS data through interfacing systems. Access to LEDS and its data will only be granted by PIAP if they are satisfied that the necessary sharing agreements and data protection compliance documentation is in place.
- A review of the data requirements of all third-party organisations with access to the PNC, or data extracted from it, has been carried out prior to those organisations being granted access to LEDS data. Organisations have been reassessed on the lawfulness, necessity and proportionality of their data access, with an emphasis on data minimisation. Restrictions may be applied to some organisations so that access to different datasets is limited.
- Users of LEDS must hold the appropriate level of Police Security Vetting Clearance. All personnel working on the LEDS programme are required to hold a high level of vetting prior to being onboarded or granted access to any LEDS system or documentation. The LEDS Vetting Policy sets out the vetting requirements for all individuals requiring access to LEDS or LEDS-derived data.
- Organisations are expected to have Local Auditors in place before accessing data from LEDS[5]. Local Auditors can access records of activities for named users undertaken during specific periods. The Audit function also enables

[5] This may be in addition to a person's existing role within the organisation.

Auditors to focus on specific criteria to review, which may be unique to their respective organisation. This will be overseen by a National Auditor, who is responsible for ensuring that Local Auditors are fulfilling their responsibilities appropriately.

Technical:

- A Security Team oversees the design and development of LEDS in accordance with industry best practice.
- The Police Digital Service (PDS) provides assurance to the PIAP and Information Asset Owner (IAO) for connecting organisations.
- LEDS is hosted on a commercial cloud platform, configured according to the PDS Police Assured Landing Zone (PALZ) technical blueprint.
- LEDS is accessed by authorised users over the Law Enforcement Community Network (LECN), a secure network for policing and Law Enforcement organisations.
- The LEDS Audit Service and Data Compliance Logging Service fulfil the legislative requirement to record the processing activities that occur across LEDS so that misuse can be deterred, located, and investigated. These tools enable a view over the interactions with LEDS Services by a given user or system. It also enables the Auditors to establish a view over what has happened and who has viewed and interacted with a given record.

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

- The LEDS Security Team determine how the Programme can effectively deliver good industry practice and monitor the implementation. The team provide advice to the Information Asset Owner (IAO) when deciding upon change and associated risk acceptance.
- The Police Digital Service (PDS) is the independent body that supports policing to deliver its digital strategy and provides second line assurance regarding information security risks. The LEDS Security Team works closely with the PDS.
- The LEDS technical solution is implementing the Information Management System (IMS), which entails the Information Security Management System (ISMS), the International Standard for Information (ISO) and the International Electrotechnical Commission (IEC) 27001. These are supported by compliance with British Standard Institute 10008 (BSI) for managing evidential weight and legal admissibility.

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

LEDS incorporates technical and organisational controls to ensure personal data is not retained longer than necessary. These include defined retention schedules, automated weeding processes, and system-generated notifications prompting data owners to review records prior to deletion.

Each LEDS Joint Controller is responsible for ensuring that data they create or manage is retained only for as long as necessary, in line with applicable retention schedules and legal obligations.

Any changes to retention schedules are subject to appropriate governance and must be authorised by the Information Asset Owner (IAO).

A review of the Retention, Redaction and Deletion (RRD) policy for the register of criminal convictions and policing data in England and Wales is currently underway. This will be replaced or updated following completion of the RRD review and implementation of the updated policy across LEDS. During the transition period where the PNC remains in operation, existing PNC retention rules will continue to apply where relevant.

Nature of the Personal Data

2k. Describe the type of personal data involved, including whether it is Criminal Offence Data[6], Special Category Data[7], or Data Subject to Sensitive Processing[8]. Where appropriate list data fields.

The personal data processed on LEDS includes Criminal Offence Data and Special Category Data, and also involves Sensitive Processing for Law Enforcement Purposes.

1. Person Service

Data from the Person Service will primarily be processed for Law Enforcement Purposes and include:

- Name, aliases, nicknames, address, telephone numbers, email address, date of birth, place of birth
- Physical descriptions, including height, hair colour, eye colour, facial features
- Sensitive data (health flags, ethnicity/race, sex, gender, warning markers)
- Criminal offence data

2. Drivers Service

The processing of data in the Drivers Service may involve both Criminal Offence Data (where details of convictions for road traffic offences are held on a person's driving licensing record) and Special Category Data (markers relating to the health of a driver). The latter will be classed as Sensitive Processing when the processing is for Law Enforcement Purposes. Data categories provided by the DVLA include:

---

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

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

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

- Driver information – photograph[9], name, address, date of birth, driver signature, eyesight/hearing restrictions and marker information
- License information
- Entitlements
- Test pass information
- Token information
- Endorsement summary
- Endorsement details

3. Vehicles Service

The processing of data in the Vehicles Service may involve both Criminal Offence Data (relating to convictions for road traffic offences) and Special Category Data (markers relating to the health of a driver). The latter will be classed as Sensitive Processing when the processing is for Law Enforcement Purposes. Vehicle data includes:

- Vehicle details
- Registered keeper details (name, address, and date since acquired)
- Previous keeper details (name, address, data from and to)
- Driver and Vehicle Licensing Agency (DVLA) markers
- Police reports and warnings
- Vehicle insurance policy details
- Details to identify whether a vehicle is correctly licensed and registered.

Free text in the report details on records may also contain references to individuals subject to the discretion of the report creator.

4. Property Service

Data in the Property Service will include the name and address, and/or other contact details (where known or available) of individuals reporting information about stolen property and / or the item's owner. The age of the individual will not be recorded in the Service, however personal data relating to children under 18 years of age will be very limited, with data concerning those under 13 years of age even more minimal. Some names are more associated with races, ethnicities or religious backgrounds than others. Location data recorded (whether it be the victim's home address, work address or incident location) may also inadvertently suggest special category links, e.g. a religious premises. Other data processed by the Property Service will include:

- Unique identifying numbers
- Make, model, colour and type of item
- Other descriptors
- Incident details

[9] A photo will not exist if a person has a paper licence issued before July 1998, has not moved address since then and is still under 70 years of age.

Some stolen or found items might indirectly identify other areas of data, e.g. health, economic situation, location/movement. Guidance will be provided to end users about handling data in such instances. The Property Service will not process Criminal Conviction Data.

5. Broadcast Service

The personal data processed in the Broadcast Service includes Criminal Offence Data and Special Category Data and relates to Sensitive Processing for Law Enforcement Purposes. Data shared within the Broadcast message may include:

- ID numbers (Unique Identifier, Broadcast request ID and PNC ID)
- Name, sex and date of birth of person
- Description of the data subject (including height, colour, marks, tattoos, clothes, etc.)
- Description of a motor vehicle, including a vehicle registration mark
- Description of an item of property

The free text function also allows users to input supplementary information into the Broadcast message which may include health data, ethnicity, warning markers, or Criminal Offence Data).

6. Interest Search Service

The Interest Search Service will store, process and present a limited set of personal data as follows:

- A 'userID' – this is the work email address of the user undertaking the initial search 'on behalf of' – this is a free text field manually entered by the LEDS user during the initial search
- Search criteria – this includes any free text fields manually entered by the user during the initial search (e.g. a Drivers licence number).

7. Data Compliance Logging Service (DCLS)

The DCLS, which captures and stores collection, alteration, disclosures, combination and erasure of data, is superseding the Disclosure Logging Service, which captures and stores disclosures only. The types and nature of personal data which may be sent to the Service is contingent upon the processing activities occurring across other LEDS Services and may contain both Criminal Offence Data and Special Category Data. DCLS does not introduce any new categories of personal data beyond those already processed by the source LEDS Services.

8. Audit Service

In addition to the personal data of a LEDS Person that the Audit search may make available (e.g. through a details search), other data available will be the personal data relating to authorised users of LEDS. This will include where they have accessed data relating to Law Enforcement processing, General Processing, Sensitive Data Processing, Special Category Data as well as Criminal Offence Data within LEDS. This

Service enables the LEDS Joint Controllers to fulfil their responsibilities under Section 62 of the DPA.

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

While from a technological perspective, LEDS will be a new service, much of the data processed is currently processed on the PNC. Therefore, PNC statistics offer insight into the expected volumes of data processing in LEDS.

As of September 2024, the PNC held approximately[10]:

- 14,079,767 Persons records
- 74,954,161 Vehicle records
- 63,996,347 Driver records (LEDS will process Driver data via an API which will not require storage, but volumes are expected to be in the region of 5.5m enquiries per annum for road traffic offences, rising significantly once the scope to use driving licensing information is extended to any Policing or Law Enforcement Purpose).

The Property Service has been fully cutover from PNC. Property items on LEDS started at around 35,000 and it is envisaged that increased future usage will allow this to grow to around 500,000.

Additional volumes are as follows:

- Broadcast - annually, an average of 1,300 broadcast messages are sent, equal to three or four a day.
- The #TE log on PNC is used for a variety of purposes and sees approximately 600,000 uses each year. LEDS has re-worked and split the #TE into three overarching areas, namely Audit, Interest Search and Search History.
- The Data Compliance Logging Service logs processing activities made on behalf of functional domains such as Person, Drivers, Vehicles, Property, Broadcast, etc. The volumes of data vary for different types of activities, ranging from a few hundred a day to 200,000 a day.

There were 192,187,671 PNC transactions for the 12 months from August 2023 – July 2024. These include search and update enquiries made on the system but do not include exports of PNC data. It is estimated that a similar number of transactions will be undertaken in LEDS once PNC is decommissioned and LEDS becomes the master data source.

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

Personal data will be processed in LEDS where it is necessary to carry out Policing and Law Enforcement duties. Under Part 3 of the DPA 2018, “Law Enforcement Purposes” are defined as “the prevention, investigation, detection, or prosecution of

[10] Data provided by PNC Customer Support team (23 October 2024)

criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." This may include:

- Protecting life and property
- Preserving order
- Preventing and investigating criminal offences
- Bringing offenders to justice
- Performing any other duty or responsibility arising from common or statute law

Where data is processed for General Purposes, the data processed is limited to that which is necessary to:

- Comply with a legal obligation
- Carry out duties in the public interest where there is a legitimate reason to do so
- Protect a Data Subject's vital interests (or the vital interests of another person).

Each Controller is responsible for producing and publishing a Privacy Notice explaining their lawful basis for processing personal data.

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

LEDS is designed with Privacy by Design as the default approach, incorporating features and controls that support the principle of data minimisation. Constrained data fields set parameters around the information users can enter, and word-count limits on free-text fields encourage the inclusion of only information that is necessary. Data is made available across distinct LEDS Services in line with user needs and entitlements, limiting visibility to information that is proportionate and lawful.

Users receive appropriate training on the lawful and proportionate handling of data within LEDS, and the Audit functionality enables authorised Auditors to monitor and review system use.

The National Police Chiefs' Council (NPCC) has appointed an NPCC LEDS Lead who chairs the Police Information Access Panel (PIAP). The PIAP considers applications from organisations seeking access to LEDS, including requests for downloads, data extracts, and access via connecting systems. Access to LEDS and its data is granted only where the PIAP is satisfied that appropriate governance, information sharing arrangements and data protection safeguards are in place.

A review of the data requirements of all third-party organisations with access to the PNC, or data extracted from it, has been carried out prior to those organisations being granted access to LEDS data. Organisations have been reassessed on the lawfulness, necessity and proportionality of their data access, with an emphasis on data minimisation. Restrictions may be applied to some organisations so that access to different datasets is limited.

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

Each Controller is responsible for the quality of its own data. They coordinate their responsibilities under a Joint Controllership Agreement, which includes several authorised organisations who will be able to create records and make updates on LEDS. This makes those organisations responsible for the quality of that data.

The personal data in LEDS is categorised, based on the scenario an individual is involved in (e.g. as a suspect or victim).

There are also design features in LEDS that reduce the likelihood of duplicate or incorrect information being entered into LEDS.

Analytical work on PNC data will determine the quality of the data against a set of agreed quality dimensions including completeness and accuracy. This will improve the quality of data that is transitioned from the PNC to LEDS.

The NPCC has reviewed performance metrics for operational use of PNC data and supporting data quality improvements.

The statutory PNC and LEDS Code of Practice has 10 principles which are underpinned by data protection principles and set out requirements including the national application of data quality standards.

Data Subjects

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

The categories of people whose data will be processed, primarily for Law Enforcement Purposes, include but are not limited to:

- A person who is the subject of a record originally created and held at the National Identification Service
- A person who has been arrested, charged or reported for summons for the commission of, or involvement in a recordable offence
- A person who is suspected of, wanted for, or convicted of, committing a specific offence
- A person who is wanted for the non-payment of fines imposed by a Court
- A person who has failed to appear at a Court in answer to a charge made against them
- A person who has been excluded from entering certain establishments by a Court
- A person who is subject of a particular type of Court Order
- A person who has absconded from, or who is subject to recall to, a detention centre, a prison, youth custody or a remand centre etc.
- A person who has deserted from the Armed Forces
- A person whose whereabouts are sought for other police purposes, e.g. as a witness to an incident
- A person who has been disqualified from driving a motor vehicle on a road by a Court.
- A person who is the subject of a roadside check to ensure their driving is in accordance with a valid driving licence entitlement
- A person who is the subject of operational information which is required to be shared nationally for policing purposes
- Owners of property (or an agent acting on their behalf), finders of property and persons reporting the loss or theft of an item of property.

Other categories of people whose data will be processed, primarily for General Processing, include but are not limited to:

- A person who has an entry on the National Firearms Licensing Management System
- A person who has been reported missing or has been found.

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

The processing of data in LEDS for Law Enforcement Purposes will not be based on consent of the Data Subjects.

The lawful basis relied upon will be that the processing is necessary for a Law Enforcement Purpose or, in the case of Sensitive Processing, done because it is strictly necessary (Part 3 Section 35(5) of the DPA).

For General Processing, one of the lawful bases under Article 6(1) of the UK GDPR may apply, such as compliance with a legal obligation, protection of vital interests, or the performance of a task carried out in the public interest.

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

The age of criminal responsibility in England, Wales & Northern Ireland is 10 years, and is 12 years in Scotland. Therefore, it is possible that LEDS will be used to process the personal details of children who are wanted, have been arrested or have been convicted of criminal offences. This is likely to be a small proportion of LEDS processing.

In the UK, a person can apply for a provisional driving licence from 15 years and 9 months old. A person can drive a moped on public roads when they are 16 years old and cars on public roads when they are 17 years old (and in some circumstances earlier). However, anyone of any age can own and/or be the registered keeper of a vehicle with the DVLA. It is therefore possible that personal data relating to persons under 18 may be processed using LEDS in relation to their driving licence information or being the registered keeper of a vehicle. Details of children may also be processed in LEDS where they have been disqualified from holding a licence.

A certificate can be granted authorising possession of a firearm, as well as acquisition (for example, by borrowing or by receiving as a gift) to a person aged over 14 years. There is no minimum age in the UK for a person to apply for a shotgun certificate. Therefore, details of minors will also be held on the National Firearms Licencing Management System (NFLMS), accessed via a LEDS interface.

Children's data will be processed in LEDS if they are the owners of stolen property, or the person reporting property as lost. This is likely to very uncommon.

Details of missing persons are processed using LEDS. This could include children and adults who may be classed as vulnerable. Urgent critical Broadcast messages containing details of vulnerable persons and missing children or children in danger will be shared to other forces, Law Enforcement Agencies and partners, specific regions and ports, to protect from potential harm, exploitation or abduction of a vulnerable person.

There may also be occasions where persons of interest (including immigration offenders and escaped prisoners) are children under the age of 18 and their details need to be included in a message sent via the Broadcast application.

Other potentially vulnerable persons whose personal details may be incidentally processed using LEDS include:

- Elderly people
- People with mental health conditions (whether temporary or ongoing)
- Asylum seekers
- Trafficked people
- Sex workers
- People forced into marriage
- People with disabilities
- Injured or chronically ill people

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

British policing is based on consent, meaning the ability of the police to carry out their functions, rests on public approval of their existence, actions and behaviour.

The existence of a national policing system such as LEDS, which processes personal data to preserve law and order, to protect the public and to keep people safe, is to be reasonably expected in a democratic society.

Information about the transition from PNC to LEDS is in the public domain. There are also published guidelines and principles on the lawful and proportionate use of personal data.

Data Subjects can exercise their data rights either directly through the relevant controller or via ACRO (whose contact details are publicly available) where such agreements with ACRO exist.

Each Controller is responsible for publishing a Privacy Notice, which informs Data Subjects about their rights and how their data is collected, processed and used.

Step 3: Consultation

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

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

External open consultation on LEDS was conducted in 2022 with members of the public prior to the PNC & LEDS Code of Practice 2023 being introduced by UK Parliament.

A consultation for the Child Rights Impact Assessment was also carried out in 2024 with children's charities, civil society organisations and young people. The assessment and recommendations have been completed.

Stakeholders have been consulted with throughout the development of LEDS, including:

- Information Commissioner's Office
- College of Policing (Training)
- Policing community
- Legal teams
- National Police Chiefs' Council (NPCC) Quality Assurance Panel
- Police Digital Service
- Information Assurance (Security) team
- NPCC Data Protection Experts
- Home Office LEDS Development Team

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

There was engagement with civil society organisations during the early development stages of LEDS.

The proposed processing will not be introducing any significant changes to the processing that has already been undertaken by Policing and Law Enforcement. As such, formal consultation is not considered necessary.

The Information Commission's Office is aware of developments and is subject to ongoing updates and dialogue with the Controllers to help shape the processing of personal data.

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

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

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

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

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

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

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
Security-related						
001: There is a risk that the Service, hosted on the Cloud, is insecure, leading to unauthorised access to personal data by internal or external users.	1 Remote	2 Significant	2 Low	Treat	The system must be hosted on a secure IT infrastructure. Ensure system security is sufficiently robust (e.g. patches maintained, authorised technical resources, performance tests, protective monitoring).	LEDS is accessed by authorised users over the Law Enforcement Community Network (LECN), a secure network for policing and law-enforcement organisations. The Service is hosted on a platform that has been independently assured by the Police Digital Service (PDS). The PDS is the key body that supports policing to deliver its digital strategy and assist with oversight of information assurance. The PDS is responsible for the security assurance of LEDS. The PDS works closely with the LEDS Security Team who identify security risks, conduct risk analysis and assessments. Secure connections are used for access to LEDS, and regular security tests are conducted. Protective Monitoring is in place to identify any security issues. The data in LEDS is held in UK data centres, and the encryption is held by the Home Office.
Access and confidentiality-related						
002: There is a risk of a technical IT or network error, or unplanned interruption to the Service, leading to the data being unavailable and/or users taking decisions on outdated data.	2 Possible	2 Significant	4 Medium	Treat	Ensure the service is as stable as possible – work with platform/cloud service suppliers.	Protective monitoring is in place to identify any security issues. Operational monitoring is also in place to ensure that remedial action is taken if the service becomes unavailable. Alerts are also generated if there is a significant increase or drop in the volume of transactions to highlight any potential issues. Incident Management processes are in place to restore lost or interrupted service as quickly as possible and track recurring issues to provide permanent solutions for persisting issues. IT Health Checks are undertaken and followed by regular ITHCs.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
003: There is a risk that entitlement rights for the Service are not appropriately managed, leading to users having access to too much or too little data.	2 Possible	2 Significant	4 Medium	Treat	Review technical, physical, or procedural measures controlling access to the information on a regular basis and amend where necessary.	The National Identity and Access Management Service (NIAM) provides a public cloud based national identity and access management service to all the police forces and other affiliated and approved UK organisations that require access to the policing systems. LEDS Entitlements are assigned via an Identity Access Management application based on the job function of the person, details of which are managed by HR. Each organisation is responsible for ensuring that appropriate entitlements are assigned to its users. No user is given access to functionality that they do not have a legitimate purpose for using. User access is disabled after a period of inactivity.
004: There is a risk that personal data from the Service is disclosed to or accessed by an unauthorised person, leading to inappropriate or unlawful use of the data.	1 Remote	2 Significant	2 Low	Treat	Educate users on how to prevent the accidental inappropriate disclosure of the information. Implement appropriate technical, physical, or procedural measures to prevent accidental disclosure of, or unauthorised access to, the information.	An organisation's access to LEDS data is managed via the PIAP process. Access will only be granted by the PIAP if they are satisfied that appropriate structures are in place to govern its use. Authorised access is managed via the National Identity and Access Management Service (NIAM), where users' entitlements are authenticated and approved. Users are required to re-authenticate their access after a period of inactivity. Any unauthorised activity on LEDS will be identified via audit (transaction monitoring) and appropriate action will be taken. Use of auditing tools will help to identify when data may have been compromised, so that steps are taken to address it and minimise further inappropriate disclosure. There are appropriate controls for Police and third-party organisations accessing LEDS data, managed by the PDS. The PNC and LEDS Code of Practice has guidance on how to use data through the application of 10 principles. Each user organisation is responsible for communicating to and training their users on the lawful and proportionate use of personal data.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
Legality-related						
005: There is a risk that the personal data processed in LEDS is used in a way which is not compatible with the purpose/s the data was initially collected for, leading to the data being used unlawfully.	1 Remote	3 Severe	3 Low	Treat	Document the lawful basis for processing personal data. Document the sharing of personal data and any legislative purpose limitations in a data sharing agreement. Audit the use of the information to identify any incompatible use, which should be stopped.	The PNC and LEDS Code of Practice has guidance on how to use data through the application of 10 principles. Each user organisation is responsible for communicating to and training their users on the lawful and proportionate use of personal data. Any sharing of LEDS data will be underpinned by a documented Data Sharing Agreement or Memorandum of Understanding which sets out the purpose and lawful basis for sharing. All user interactions on LEDS will be logged, along with the relevant processing activities which meet the requirements under Section 62 of the DPA. National Auditors will audit logs to identify misuse and proactively manage any deviation of the use of data outside of permitted purposes. Local audit processes are also in place.
006: There is a risk that the personal data from the Service is used by an authorised person for unauthorised purposes, leading to the data being used for personal, malicious and/or criminal reasons.	2 Possible	3 Severe	6 Medium	Treat	Document the approved uses for which an enquiry can be made against that information. Audit the use of the information to identify any incompatible use, which should be stopped.	Police and Law Enforcement users have strict Codes of Practice. All authorised users of the Service must be currently vetted against the appropriate standards in accordance with their data access level. The LEDS Vetting Policy sets out the vetting requirements for all individuals requiring access to LEDS or LEDS-derived data. Data Sharing Agreements also contain information about the required vetting and clearance for users. The PNC and LEDS Code of Practice has guidance on how to use data through the application of 10 principles. Each user organisation is responsible for communicating to and training their users on the lawful and proportionate use of personal data. All users must read, understand, and comply with the Security Operating Procedures (SyOPs), where one exists, before accessing the Service. Prior to executing a search in LEDS, users must provide a reason code and justification before progressing on to use the data. Local Auditors carry out audits of user actions in LEDS. National Auditors will audit access logs to ensure compliance with use of data for permitted purposes, identify misuse and proactively manage any deviation of local audit processes.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
007: There is a risk that the various legal frameworks of the Joint Controllers will not be designed into LEDS, leading to data not being processed in accordance with the laws of each jurisdiction.	2 Possible	2 Significant	4 Medium	Treat	Clarify the technical solutions for managing instances of other jurisdictions. Work closely with impacted stakeholders including (but not limited to) Police Scotland & Police Service of Northern Ireland. The legal framework governing data quality, retention, and Data Subjects' rights must be complied with.	The Data Protection Act 2018 requires each (Joint) Controller to regularly review personal data and ensure it is retained only for as long as necessary for the purposes for which it is processed, in accordance with applicable legislation and relevant national or local policies and guidelines. This may be different for different parts of the UK. Under the LEDS Joint Controllership Agreement (JCA), it has been agreed that the NPCC LEDS Lead can implement a Retention, Redaction & Deletion (RRD) policy for LEDS while ensuring that Weeding and Retention policies and legislative requirements of other jurisdictions are adhered to. It also states that any RRD policy must not override the requirements of other jurisdictions. Each Jurisdiction's rules and regulations are being managed within the development of LEDS. For example, LEDS uses unique Offence Codes to differentiate current and historical offences that come from the six geographical areas, namely England & Wales, Scotland, Northern Ireland, Guernsey, Isle of Man and Jersey.
008: There is a risk that the Service is designed without due regard to the Equality Act 2010, leading to data relating to people with a protected characteristic being used unfairly, and/or in a biased and discriminatory way.	1 Remote	2 Significant	2 Low	Treat	Implement measures to ensure that the design of LEDS does not lead to the information being used to inappropriately discriminate against certain groups, particularly children. The 9 Equality Act Protected Characteristics are: Age, Sex, Pregnancy and maternity, Marriage and Civil Partnership, Gender Reassignment, Sexual Orientation, Race, Religion or belief, Disability.	The Home Office must comply with the Public Sector Equality Duty (PSED) under Section 149 of the Equality Act 2010. The PSED aims to ensure public bodies play their part in tackling discrimination and inequality and contribute to making society fairer. An Equality Impact Assessment (EIA) is the current method to demonstrate that proportionate due regard has been considered, and one has been produced for LEDS and published on the Gov.uk website. The Home Office LEDS Developers were consulted and engaged in the assessment process to ensure potential inequalities were flagged at an early stage in its development. The EIA will continue to evolve as decisions are made about the features and components for the Service and will be published at regular intervals. A core part of requirements was to identify national data sources that were used to form evidence and facilitate greater understanding about policing and the 9 protected characteristics. A Child Rights Impact Assessment has been carried out to better understand any potential risks to children so they can be mitigated and developed into LEDS as part of its design.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
009: There is a risk that the Service may not incorporate features designed to protect the data of vulnerable people and/or children, leading to adverse impacts to those affected.	2 Possible	2 Significant	4 Medium	Treat	Implement measures to ensure that the design of LEDS does not lead to the information being used to inappropriately discriminate against certain groups, particularly children.	A Child Rights Impact Assessment has been carried out to better understand any potential risks to the use of children's data, so they are mitigated and developed into the service as part of its design. An Equality Impact Assessment has also been undertaken as a tool to identify and address any negative impact that the Service may have on those with protected characteristics. An Integrated Management System (IMS) is being developed to provide structure and governance for the quality and security of LEDS Data and Operational Police Services. LEDS has also been certified to British Standards with BS10008. This provides even greater confidence as this certification sets the standards for the evidential weighting and legal admissibility of the Service.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
Governance-related						

010: There is a risk that the Service has inadequate governance structures in place, leading to organisations mismanaging access to and/or use of personal data.	1 Remote	2 Significant	2 Low	Treat	Implement and maintain necessary policy or procedure concerning the access or use of the information.	LEDS is accessed by authorised users over the Law Enforcement Community Network (LECN), a secure network for policing and Law Enforcement organisations. NIAM is an access broker allowing direct LEDS users within the Law Enforcement Community to access national applications through a single sign-on. The management of direct LEDS user access is carried out by Federated Identity Providers within the user organisations, such as Police Forces or other government bodies. Applications for access to LEDS data by non-police organisations are subject to a transparent approval process. The National Police Chiefs' Council (NPCC) has elected a NPCC LEDS Lead who is responsible for chairing the Police Information Access Panel (PIAP), which considers applications from organisations for access to the Service. The PIAP also considers requests for systems which access LEDS data through interfacing systems, downloads or extracts. This PIAP process includes applications from wider Law Enforcement, and from some commercial organisations to allow them limited access to redacted or filtered data, for use in applications that support Law Enforcement Purposes. Approval to access the Service and its data will only be granted by the PIAP if they are satisfied that appropriate structures are in place to govern its use. This includes having the necessary sharing agreements and data protection compliance documentation in place. A review of the data requirements of all third-party organisations with access to the PNC, or data extracted from it, has been carried out prior to those organisations being granted access to LEDS data. Organisations have been re-assessed on the lawfulness, necessity and proportionality of their data access. Users are only granted access which is relevant to their job function and are not given access to any functionality that they do not have a legitimate purpose for using. Authorised Professional Practice on data protection has been produced to assist police forces with their statutory responsibility to comply with the DPA 2018 and UK GDPR. A separate, more detailed NPCC Data Protection Manual of Guidance has been produced for police data protection professionals. The statutory PNC and LEDS Code of Practice sets out guidance on the use of data through the application of ten principles. Where law enforcement agencies or government departments are granted access to LEDS, either directly or via an interface, but are not legally bound by the statutory Code, compliance is required through a written agreement between those organisations and the LEDS Joint Controllers. LEDS has also been certified to British Standards with BS10008. This provides even greater confidence as this certification sets the standards for the evidential weighting and legal admissibility of the Service.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
011: There is a risk that the Service does not have the necessary agreements and data protection documentation in place, leading to personal data in LEDS not being properly safeguarded.	1 Remote	2 Significant	2 Low	Treat	Implement and maintain necessary information sharing agreements and data protection compliance documents, and review these regularly.	There is a process in place for the completion of Data Sharing Agreements and compliance documents required under the Data Protection Act 2018 and UK GDPR. This process is coordinated by data protection and policy experts in the Home Office and Policing. The Police Information Access Panel (PIAP) considers applications for access to LEDS, including any requests for downloads and data extracts. PIAP also considers requests for systems which access LEDS data through interfacing systems. Access to LEDS and its data will only be granted by PIAP if they are satisfied that the necessary sharing agreements and data protection compliance documentation are in place.
012: There is a risk that the Service is not designed to comply with logging requirements under Section 62 of the Data Protection Act 2018, leading to non-compliance with data protection legislation.	2 Possible	2 Significant	4 Medium	Treat	Understand the implications of accessing APIs on s62 and Data Access Rights. Determine the gaps that exist between Audit product and API data processing. Implement measures to ensure that logs are kept when information is collected, altered, shared, combined or erased.	Logging capability is being designed into LEDS to fully meet the requirements set out in Section 62 of the DPA. The system will apply the same logging to all processing activities undertaken by LEDS users. The LEDS Audit Service and Data Compliance Logging Service fulfil the legislative requirement to record the activity that occurs across LEDS so that misuse is deterred, located, and investigated. The tool enables a view over the interactions with LEDS services by a given user or system. It also enables the auditors to establish a view over what has happened and who has viewed and interacted with a given record.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
Data Quality-related						
013: There is a risk that the integrity of the Service is affected by personal data being inaccurate, incomplete or of poor quality, leading to adverse decisions being made.	2 Possible	2 Significant	4 Medium	Treat	Document arrangements pertaining to data quality.	Responsibility for data quality lies with the Controller that initially creates each record. LEDS functionality will enable user organisations to review, amend and ultimately delete records stored within LEDS. It is recognised that the LEDS Joint Controllers will not have control of some of the data being processed via LEDS. In particular, the Drivers and Vehicles Services access data under the controllership of the DVLA, DVSA and MIB, and therefore the LEDS Joint Controllers are reliant on those other organisations to provide accurate and complete data. However, if a LEDS Joint Controller is not satisfied that correct data has been shared by those organisations, it should not be used. The statutory PNC and LEDS Code of Practice has 10 principles which are underpinned by data protection principles and set out requirements including the national application of data quality standards. They emphasise the importance of high-quality data, the accuracy and relevance of data and the need for rectification should any inaccuracies be identified. LEDS has also been certified to British Standards with BS10008. This provides even greater confidence as this certification sets the standards for the evidential weighting and legal admissibility of the Service. There is work in progress to ensure that the data fields in LEDS are aligned with those in PNC when data is migrated across.
014: There is a risk that during the dual running of both PNC and LEDS, errors occur which mean the data is not synchronised as expected, leading to adverse decisions being made on outdated data.	1 Remote	3 Severe	3 Low	Treat	Ensure the replication process is sound between the services before roll-out.	The development of LEDS is following a defined governance testing cycle. This includes functional, performance, regression, user acceptance and defect testing phases. Permission will be sought by the NPCC LEDS Lead via an Approval to Proceed where required. Individuals from pilot organisations are being used to ensure the quality of the Service as a part of this testing process, which reduces the risk that LEDS does not meet requirements.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
Records Management related						
015: There is a risk that the Retention, Redaction and Deletion (RRD) policy for LEDS will not be implemented before PNC is decommissioned, leading to unlawful processing of personal data.	2 Possible	2 Significant	4 Medium	Treat	Review and apply approved RRD policy for England, Wales, Scotland, Northern Ireland and the Crown Dependencies.	The LEDS Joint Controllers have commissioned a formal review of RRD to ensure that a defined policy is in place before PNC is decommissioned. Subject Matter Experts are also being consulted, e.g. those that have designed and managed RRD systems and processes for Police Forces. Rigorous testing will ensure that data is not deleted prematurely, and an exception report will advise Controllers/Owners of records when there are data quality issues that prevent the RRD system from disposing according to the schedule.
Training and user capability related						
016: There is a risk that authorised users of the Service are inadequately trained, leading to inappropriate or unlawful use of personal data.	1 Remote	2 Significant	2 Low	Treat	Implement appropriate training for all users.	Each user organisation is responsible for communicating to and training their users on the lawful and proportionate use of personal data. These are not new arrangements so organisations should already have processes in place for this. The PNC and LEDS Code of Practice has guidance on how to use data through the application of 10 principles. A Code of Practice Learning Programme has been developed for existing users of PNC and LEDS to undertake prior to using LEDS, which will ensure that they are aware of legal and operational obligations. Auditors will receive audit specific training above and beyond the training for standard users. All users must read, understand, and comply with Security Operating Procedures (SyOPs), where one exists within their organisation, before accessing LEDS.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
017: There is a risk that LEDS users will not be able to identify the age or category of Data Subjects leading to erroneous decisions being taken in relation to those individuals.	2 Possible	2 Significant	4 Medium	Treat	Ensure that LEDS is designed to identify the different categories of data subjects. Ensure clarity of data source is maintained. Maintain regular interaction with the product teams to ensure data is kept separate for wider law enforcement processing to avoid the data belonging to missing/vulnerable people, who are often children, being merged with criminal data enquiries. Ensure that LEDS is developed to promote accuracy of checks, including pre-population fields. Provide sufficient training to all users on managing data subject categories and interpreting search results.	LEDS is being developed to ensure that classifications are clearly defined to meet legislation requirements, e.g. Offenders and Suspects will be classified according to what events they are linked to. A date of birth capture is already a field in PNC, and this has been replicated in the LEDS (Person) design. A Child Rights Impact Assessment has been carried out to better understand any potential risks to children, so mitigations are developed into the service as part of its design. It will be clear to users what classifications of data are produced when using each LEDS Service. All data captured in LEDS will be classified. However, any free text data migrated as part of Property Service from PNC may not be classified in terms of Data Subject categories and ages.

1. Information Risks	2. Likelihood of harm (1 Remote, 2 Possible, 3 Probable)	3. Severity of harm (1 Minimal, 2 Significant, 3 Severe)	4. Overall Risk (1-3 Low, 4-6 Medium or 7-9 High) derived from multiplying likelihood and severity	**5. Decision (Terminate, Tolerate, Transfer or Treat)**	**6. Potential Risk Treatment**	**7. Risk Treatment to be adopted, or comments**
Miscellaneous						
018: There is a risk that Data Subjects will be unaware of their rights in respect of their personal information, leading to Data Subjects potentially not exercising those data rights.	1 Remote	2 Significant	2 Low	Treat	Ensure that Privacy/Fair Processing Notices provide details of Data Subjects' rights and how to exercise them.	Separate privacy notices are published by individual Controllers of the data, which detail all Data Subject rights. PACE Codes of Practice and Authorised Professional Practice documents for Policing set out obligations on the police under the DPA 2018 and are available online to members of the public. Data Subjects are entitled to exercise their rights through any of the LEDS Controllers. The Joint Controllers of the Service based in England, Wales and Northern Ireland have appointed ACRO Criminal Records Office (ACRO) to manage Subject Access Rights applications to LEDS on their behalf, and Data Subjects are encouraged to use their processes. Police Scotland directly discharges its own responsibilities in relation to Data Subject Rights. The LEDS Data Protection Policy has been published on the GOV.UK website which contains details about how Data Subjects can exercise their data rights. This DPIA is also published on the GOV.UK website which will help Data Subjects understand how data is being used within LEDS.

Annex A: LEDS DPIA Glossary

ACRO Criminal Records Office (ACRO)	With the permission of the police forces in England and Wales, ACRO provides PNC information to organisations which do not have direct access to PNC/LEDS. It is also the lead organisation for Data Subject Access Requests made to England and Wales police forces and the UK Central Authority for the Exchange of Criminal Records. As the UKCA-ECR, it is the conduit through which criminal record exchange happens between the UK and other countries, predominantly, but not exclusively EU member states.
Amazon Web Services (AWS)	Cloud-service provider hosting and enabling access to LEDS.
Application Programming Interface (API)	A set of rules and protocols that allow different software applications to communicate with each other. In LEDS, APIs allow access to data held by third-party organisations such as the DVLA, MIB and DVSA.
BS10008	British Standard on evidential weight and legal admissibility of electronically stored information. The LEDS Service has accreditation for this standard.
College of Policing	A professional body in England and Wales for those working across policing. It is an operationally independent non-departmental public body.
(Joint) Controller	For example, a company or public authority) which determines the purposes and means of the processing of personal data.
Crown Dependency	Jersey, Guernsey and the Isle of Man. The Crown Dependencies are not part of the UK but are self-governing dependencies of the Crown. They have their own legislative assemblies, administrative, fiscal and legal systems. They are third countries for Data Protection purposes.
Data Processing Contract (DPC)	A contract, between one or more controllers and a processor who is processing data on their behalf, setting out obligations for controllers and processors. One exists between the LEDS Joint Controllers and the Home Office.
Data Protection Act 2018 (DPA)	An Act making provision for the regulation of the processing of information relating to individuals. Part 3 of the DPA covers processing by competent authorities for Law Enforcement Purposes and is the data protection regime for most of the processing taking place on LEDS.
Data Protection Impact Assessment (DPIA)	A document assessing the impact of processing operations on the protection of personal data. One must be done for processing that is likely to result in a high risk to the rights and freedoms of individuals.
Data Subject	The identified or identifiable living individual to whom personal data relates (Section 3(5) of the DPA).
Driver and Vehicle Licensing Agency (DVLA)	Agency responsible for managing UK vehicle registration details and the Great Britain driving licence issuing body. Controller of the data they share with LEDS.
Driver and Vehicle Standards Agency (DVSA)	Agency administering driving tests and MOTs in Great Britain. Controller of the data they share with LEDS.

Entitlements	The set of specific privileges that are assigned to an individual or system.
Home Office	The central government department, which is responsible through Home Office Digital, for developing the LEDS Service.
Information Asset Owner (IAO)	Also known as the NPCC LEDS Lead.
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information Technology Health Check (ITHC)	IT security assessment required, as part of an accreditation process, for many government computer systems in the UK.
IS0/IEC 27001	The information security standards which will also be utilised, jointly with BS10008, as an integrated management system.
Joint Controller Agreement (JCA)	Arrangements put in place by Joint Controllers to satisfy the obligations placed upon them by Section 58 of the DPA and Article 26 of the UK GDPR in respect of their Joint Processing of Personal Data. There is a JCA for Policing and Law Enforcement, which includes the nomination of the NPCC LEDS Lead.
Law Enforcement Community Network (LECN)	A secure network used by UK law enforcement to access national policing systems and share information.
LEDS Programme	A Programme delivering the replacement of PNC with a Service that provides equivalent (or Parity) functionality. The LEDS programme will provide a set of extensible products/services capable of delivering major transformation in the future.
Managed File Transfer (MFT)	A method for sending files (extracts) from LEDS to authorised organisations, including policing. All files will be encrypted in transit.
Management of Police Information (MOPI)	Statutory code of practice on the management of police information, introduced in 2005, in direct response to recommendations of the Bichard enquiry report. Recently replaced by the Police Information and Records Management Code.
Memorandum of Understanding (MOU)	A non-legally binding agreement entered into by government departments, as they cannot enter into formal contracts with each other.
Motor Insurers' Bureau (MIB)	MIB manages a database of car insurance data using the Motor Insurance Database (MID).
NASCH	Name, Age, Sex, Colour and Height.
National Crime Agency (NCA)	The UK's lead agency against organised crime; human, weapon and drug trafficking; cybercrime; and economic crime that goes across regional and international borders. Part of the LEDS Joint Controllership Agreement as a Law Enforcement organisation.
National Firearms Licensing Management System (NFLMS)	A database holding details of all persons who have applied for, or have been granted, a certificate for a firearm or shotgun, or who have ever applied for such a certificate, or had their certificate revoked.
National Identity and Access Management (NIAM)	The authentication platform used to confirm a user's identity.

National Police Chiefs' Council (NPCC)	Provide direction in policing and drive progress for the public.
Non-Police Organisation	An organisation granted access by the Controllers (either directly or indirectly) to LEDS data in support of policing objectives, including safeguarding.
Part 2 DPA 2018	Together with the UK GDPR, the regime applying to the general processing of personal data.
Part 3 DPA 2018	The section of the Data Protection Act 2018 applying to competent authorities' processing of personal data for a Law Enforcement Purpose.
Personal Data	Any information relating to an identified or identifiable living individual.
Photos at the Roadside (PARS)	An application which allows police officers to access driver licence photographs held on DVLA's driver database through their mobile devices.
PNC and LEDS Code of Practice	A statutory Code of Practice and guidance setting out the basic principles in relation to the ethical and professional processing of data and information managed through PNC and LEDS.
Police Digital Service (PDS)	The UK organisation responsible for coordinating, developing, delivering, and managing digital services and solutions that enable UK policing to safely harness technology to improve public safety. It provides security assurance of LEDS.
Police Information Access Panel (PIAP)	The NPCC committee responsible for dealing with applications for non-police organisation access to PNC and LEDS.
Police Information and Records Management	Statutory Code of Practice and guidance setting out national principles for police information and records management.
Police Interfaces	A method by which a local force system can interact with the PNC/LEDS.
Police National Computer (PNC)	The current UK national Law Enforcement database which is the main central record of an individual's criminal convictions. It also captures data relating to missing people, vehicles, driving licenses and stolen property. It is due to be de-commissioned in 2026 and replaced by LEDS.
Police National Computer Identification number (PNC ID)	A unique system generated reference number issued to each record in the PNC Names database.
Police Service of Scotland	The single territorial police force for Scotland. Through National Systems Support, it delivers the Criminal History System, Scottish Intelligence Database, and other Scottish policing systems.
Privacy Notice	A document outlining how an organisation processes personal data and how individuals can access their data rights. It can typically be found on an organisation's website.
Processing (data)	Processing means using personal data in any way, including collecting, storing, retrieving, consulting, disclosing or sharing with someone else, erasing, or destroying personal data.
Processor	An organisation processing personal data on behalf of the Controller.
Public Cloud-based Platform	A third-party provider that delivers computing resources over the Internet.
Retention, Redaction & Deletion (RRD) Policy	The policy setting out how long personal data should be retained. This is currently being reviewed by policing.

Section 62 DPA (Law enforcement logging)	A requirement in Section 62 of the DPA that there must be a record of the collection, alternation, consultation, disclosure (including transfers), combination and erasure of processing operations in automated processing systems. LEDS will use the Audit service and the Data Compliance Logging Service to meet their Section 62 obligations.
Transaction Enquiry (#TE)	This code is used in PNC to undertake high-level transaction log enquiries, e.g. as a Transaction Auditing Tool to search over a prescribed time period for the previous day, and/or a prescribed geographic area of the organisation.
UK GDPR	The United Kingdom General Data Protection Regulation (UK GDPR) sets out the data processing rules for data being processed for general purposes (i.e. not for Law Enforcement Purposes).
User (LEDS)	An individual who has access to LEDS data. The PIAP will be responsible for reviewing requests for access to LEDS.
Warning Markers	Markers used on police systems to identify where an individual may pose a risk to themselves, pose a risk to others, be vulnerable or be wanted in connection to an offence.