Home Office

NPCC
National Police Chiefs' Council

Law Enforcement Data Service (LEDS)

Data Protection Policy

Document owner
Version No: 1.0
Issue Date: 10 December 2025

Related Document Index

Related Document name	Location
LEDS Data Protection Impact Assessment	Will be published on GOV.UK
Equality Impact Assessment	Law Enforcement Data Service: equality impact assessment - GOV.UK
Child Rights Impact Assessment	LEDS Child Rights Impact Assessment (CRIA) - GOV.UK
Code of Practice for the Police National Computer (PNC) and Law Enforcement Data Service (LEDS)	Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) (accessible) - GOV.UK
NPCC Data Protection Manual of Guidance	Available to authorised users who are logged onto the Knowledge Hub and are members of the NPCC Data Protection Knowledge Hub Group.

Next review

This policy is recommended to be reviewed annually or sooner if there is a major change that requires the policy to be updated.

The Freedom of Information Act

The Freedom of Information Act (2000) is a law that gives the public the right to access information held by public authorities. All UK-based police forces and public organisations using LEDS are separate public authorities subject to this Act, as is the Home Office.

Contents

1. Background

The Law Enforcement Data Service (LEDS) is a national policing information system designed in collaboration between policing and the Home Office to replace functionality provided by the Police National Computer (PNC) for more than 50 years by using modern, cloud-based services being developed by the Home Office to replace the existing Police National Computer (PNC) in the UK. It aims to provide a unified, comprehensive data service that enhances the ability of law enforcement agencies to access and share information efficiently, and will streamline law enforcement operations, making them more efficient and effective in protecting the public.

LEDS draws together data from local and national policing systems, providing an inherent set of data, for which the Police and Law Enforcement Agencies (LEAs) are responsible. LEDS also connects with a variety of external organisations through interfaces, enabling both the receipt of data from other sources and the sharing of relevant information with authorised third parties.

LEDS comprises a number of national datasets (services) of Policing and Law Enforcement information and interfaces to information held by other agencies, which is available to all police forces throughout the United Kingdom. In addition, other LEAs and non-LEA organisations (non-LEAs) may also be given access to data by the LEDS Joint Controllers to prevent and investigate crimes and/or fulfil their public safety functions.

LEDS is being developed within the requirements of Data Protection legislation, including adopting privacy by design and default. Compliance with the legislation is being ensured through assurance mechanisms built into LEDS development.

2. Purpose and Scope

The purpose and scope of this document is to establish a policy that sets out how those statutory obligations relating to the management of personal data in LEDS arising from the Data Protection Act 2018 (DPA) and United Kingdom General Data Protection Regulations (UK GDPR) will be addressed. It defines the expectations for lawful and compliant handling of personal data accessed via LEDS, in line with Data Protection principles.

Each organisation involved in the processing of LEDS data is expected to maintain its own policies and procedures relating to data protection, records management, and associated governance requirements. This policy document is not intended to supersede or replace any existing organisational policies, but rather to complement them by providing overarching guidance relevant to LEDS operations.

Once the Police National Computer (PNC) is decommissioned, LEDS will become the master data source for national policing and law enforcement information. This policy supports that transition by establishing a consistent

framework for the lawful and compliant handling of personal data within LEDS, in accordance with applicable Data Protection legislation.

The LEDS Policy and Compliance Team is responsible for the efficacy of this policy document which will be reviewed annually, or earlier if required.

3. Roles and Responsibilities

3.1 Controllers

A core set of Controllers have entered into a Joint Controllership Agreement (JCA) for the processing of data within LEDS. The JCA represents the obligations placed upon the Joint Controllers by Section 58 of the DPA and Article 26 of the UK GDPR in respect of their joint processing of personal data within LEDS. The agreement covers the 43 geographical police forces of England and Wales, British Transport Police, Civil Nuclear Constabulary, Ministry of Defence Police, Police Service of Scotland, Police Service of Northern Ireland (PSNI) and the National Crime Agency (NCA). Any data entered onto LEDS by any of the Joint Controllers will become the subject of the Joint Controllership.

Outside the JCA, other organisations are considered as Controllers of LEDS processing if they store or update their own data within LEDS and remain accountable for their own processing within the infrastructure that they share with the Joint Controllers.

Some data stored outside of LEDS but accessed via LEDS (i.e. Vehicles and Drivers data) is under the controllership of other agencies and organisations such as the Driving and Vehicle Licensing Agency (DVLA), the Driver and Vehicle Standards Agency (DVSA) and the Motor Insurers' Bureau (MIB). Once a LEDS user organisation receives data, it becomes a Controller for that data. Memoranda of Understanding exist between those parties setting out the sharing arrangements between the Controllers of that data.

Other non-police and third-party organisations may be granted access by the LEDS Joint Controllers (either directly or indirectly) to LEDS data in support of policing objectives, including safeguarding. When data is shared with another organisation within the terms of a sharing agreement, they assume controllership of their copy of the personal data disclosed to them.

Each organisation that handles data in LEDS is responsible and accountable for compliance with the DPA and UK GDPR (or other relevant laws if they are outside of the UK).

Controllers must individually ensure their own police force or organisation are compliant with Data Protection legislation.

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

Each Controller is individually responsible for complying with any registration or fee-paying requirements with its Data Protection supervisory authority which, in the UK, is the Information Commissioner's Office.

3.2 Lead Controller

The Lead Controller for LEDS is authorised to act on behalf of the Joint Controllers within the terms of the JCA. This includes being authorised to enter into any data sharing or processing arrangements on behalf of each of the Joint Controllers.

3.3 National Police Chiefs' Council (NPCC) LEDS Lead

The Lead Controller has designated the NPCC LEDS Lead to ensure that Data Protection compliance activities take place in respect of LEDS on behalf of the Joint Controllers. The role and responsibilities of the NPCC LEDS Lead are set out under the terms of the JCA.

3.4 Processors and Sub-Processors

The Joint Controllers will ensure that the requirements of Chapter 4, Part 3 of the DPA 2018 are met in relation to the use of a Processor or Sub-Processor for the Processing of the Data in LEDS.

The Home Office is responsible for providing the IT infrastructure for LEDS. The LEDS Joint Controllers have appointed the Secretary of State for the Home Department (the SSHD) as a Processor to undertake certain processing activities as determined by and on behalf of the Joint Controllers. The SSHD as a Processor is subject to Home Office policies.

The Joint Controllers have authorised the SSHD to assign sub-processors, as required. The SSHD has appointed Amazon Web Services UK Branch as a sub-processor, to provide the cloud-hosting services.

Data agreements will be used to manage specific data responsibilities and accountability, including Data Processing Contracts to define the relationship between policing and the Home Office, as well as other sub-processors.

3.5 System Users

System users are police or non-police personnel with permitted entitlements to view, amend, and/or delete data held within, or accessed via, LEDS.

System users must adhere to the ten principles in the Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS), which are underpinned by current Data Protection principles. The accompanying LEDS guidance document provides detail on how system

users can support their chief officers in complying with the requirements of the Code.

Each user organisation is responsible for communicating to and training their system users on the lawful and proportionate use of personal data. Learning programmes have been developed for system users to ensure they are aware of their legal and operational obligations. An operational training package will also be provided to new system users to emphasise the importance of good quality data, accuracy and relevance of the personal data they process.

Individual system users of LEDS will assume personal responsibility for managing data in accordance with statutory obligations arising from the DPA and the UK GDPR and identifying and reporting matters requiring consideration to the NPCC LEDS Lead.

4. Data Protection Regimes

LEDS is primarily designed to support processing for law enforcement purposes, in accordance with Part 3 of the DPA. However, it also supports processing for general purposes (for example missing persons or vetting), in accordance with UK GDPR and Part 2 of the DPA.

All LEDS Controllers or other user organisations need to be clear about which regime they are engaging for each of their processing operations.

5. Data Protection Principles

The LEDS Joint Controllers have a duty to ensure that all personal data is processed in accordance with the principles set out in the Data Protection Act 2018, specifically under Part 2 (General Processing) and Part 3 (Law Enforcement Processing).

Part 3 Law Enforcement Processing (Sections 35–40 of the DPA 2018)

Where personal data is processed for law enforcement purposes by competent authorities, the following principles apply:

1. **Lawfulness and Fairness**
   Data must be processed lawfully and fairly. *(Section 35)*
2. **Purpose Limitation**
   Data must be collected for specified, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes. *(Section 36)*
3. **Data Minimisation**
   Data must be adequate, relevant, and not excessive in relation to the purpose for which it is processed. *(Section 37)*
4. **Accuracy**
   Data must be accurate and, where necessary, kept up to date. *(Section 38)*

5. **Storage Limitation**
   Data must not be kept in a form which permits identification of data subjects for longer than necessary. *(Section 39)*
6. **Security**
   Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. *(Section 40)*

Part 2 General Processing (UK GDPR Article 5)

The following principles apply to all personal data processed under general purposes:

1. **Lawfulness, Fairness and Transparency**
   Personal data must be processed lawfully, fairly, and in a transparent manner. *(Article 5(1)(a))*
2. **Purpose Limitation**
   Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. *(Article 5(1)(b))*
3. **Data Minimisation**
   Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. *(Article 5(1)(c))*
4. **Accuracy**
   Data must be accurate and, where necessary, kept up to date. Inaccurate data must be rectified or erased without delay. *(Article 5(1)(d))*
5. **Storage Limitation**
   Data must be kept in a form which permits identification of data subjects for no longer than is necessary. *(Article 5(1)(e))*
6. **Integrity and Confidentiality (Security)**
   Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. *(Article 5(1)(f))*
7. **Accountability**
   The Controller is responsible for, and must be able to demonstrate, compliance with all of the above principles. *(Article 5(2))*

6. Lawful basis for processing data

The processing of personal data within LEDS is governed by both Part 2 and Part 3 of the Data Protection Act 2018 (DPA), depending on the purpose of the processing.

Part 3 Law Enforcement Processing

Under Part 3 of the DPA, personal data is processed where it is necessary for a law enforcement purpose[1], or in the case of sensitive processing[2], done because it is strictly necessary (DPA Part 3 Section 5(5)).

For sensitive processing, the lawful basis must meet the strict necessity requirement under Section 35(5), and one of the conditions in Schedule 8 must also apply (e.g. statutory purpose, administration of justice, vital interests, safeguarding, or fraud prevention).

Part 2 General Processing

Under Part 2 of the DPA and Article 6(1) of the UK GDPR, personal data may be processed on the basis of:

- Legal obligation
- Vital interests
- Public task

Each Controller is individually responsible for determining and documenting the lawful basis they rely upon for each processing activity. This must be clearly recorded in a Privacy Information Notice (PIN) and made publicly available.

7. Special Category Data and Sensitive Processing

The personal data processed in LEDS includes criminal offence data[3] and special category data[4]. Criminal offence data is not special category data; however, it does have protections under Data Protection legislation.

When undertaking sensitive processing for a law enforcement purpose, one of the following conditions in Schedule 8 of the DPA must be met:

- Statutory purpose
- Administration of Justice
- Protecting an individual's vital interests
- Safeguarding children and those at risk
- Preventing fraud

[1] Defined in Part 3 Section 31 of the DPA as "The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety."

[2] Defined in Section 35(8) of the DPA as the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, a person's sex life or sexual orientation.

[3] Defined in the UK GDPR as personal data relating to criminal convictions and offences or related security measures.

[4] Defined in the UK GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, a person's sex life or sexual orientation.

Sensitive information, which does not meet the definition of special category data, but is deemed sensitive, may require additional handling arrangements.

Relevant controllers implement and maintain appropriate policy documentation covering the processing of special category/sensitive data as a requirement under Part 3, Section 42 of the DPA.

8. Children and vulnerable people's data

There may be occasions where the personal data of children and/or vulnerable individuals' data will be processed in LEDS.

A Data Protection by design and by default approach has been adopted to ensure that privacy and Data Protection issues are considered during the design and development stages of LEDS. This has enabled design features to be incorporated into LEDS which will safeguard and protect the rights of children and vulnerable people whose data is processed in LEDS.

Children are entitled to specific protection regarding their personal data. 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 aims to balance the benefits of improved data management for law enforcement with the need to protect children's rights, ensuring that their voices are heard and their data is handled with care. The CRIA is intended to demonstrate compliance with the United Nations Convention of Right of a Child (UNCRC)[5] and is deemed good practice.

The Home Office, responsible for providing the IT infrastructure for LEDS, 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 consideration has been given to the impact of policies and programmes on people who share protected characteristics[6]. An EIA has been undertaken for LEDS and is available on the GOV.UK website. The EIA will be periodically reviewed to ensure any decisions are taken with an understanding of potential and unintended impacts on individuals with protected characteristics.

The Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) 2023 addresses the processing of data to safeguard children and vulnerable adults.

[5] The UNCHR is an international human rights treaty that grants all children and young people (aged 17 and under) a comprehensive set of rights. The UK signed the convention on 19 April 1990, ratified it on 16 December 1991 and it came into force on 15 January 1992.

[6] Defined by Chapter 1 of the Equality Act 2010 as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

The LEDS DPIA 2025 also assesses the impact of processing operations on the protection of personal data belonging to children and vulnerable people, and mitigations have been put in place to manage any identified risks.

9. Data Accuracy

Each Controller is responsible for the quality of its own data including the creation of, and updates to, new and existing records on LEDS.

Where LEDS Services access data under the controllership of the DVLA, DVSA and MIB, the LEDS Joint Controllers are reliant on those other organisations to provide accurate and complete data.

The statutory Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) 2023 has ten principles which are underpinned by Data Protection principles and set out requirements including the national application of data quality standards.

A supporting Code of Practice Learning Programme has been produced for all LEDS users to emphasise the importance of good quality data, accuracy and relevance of data and the need for rectification should any inaccuracies be identified.

To improve the quality of data that is transitioned from the PNC to LEDS, Operational Quality checks and Data Quality Specification tests are being undertaken to determine the quality of the data against a set of agreed quality dimensions, including completeness and accuracy.

Operational data recorded in LEDS is also covered by the Code of Practice on Police Information and Records Management (PIRM) 2023, which promotes strong data governance and ensures the integrity and quality of both the system and the data it processes.

10. Data Access

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 LEDS.

All authenticated users will be able to access the data needed to fulfil their operational needs using password protected and authorised devices, as per the LEDS entitlements assigned via an Identity Access Management application based on the job function of the person.

Applications for access to LEDS data by organisations other than the LEDS Joint Controllers are subject to a transparent approval process. The National Police Chiefs' Council (NPCC) has elected a NPCC LEDS Lead who is responsible for chairing, on behalf of the Joint Controllers, the Police Information Access Panel (PIAP) which considers applications from

organisations for access to LEDS. The PIAP also considers requests for systems which access LEDS data through interfacing systems, downloads or extracts.

The PIAP process includes applications from wider law enforcement and also 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 LEDS 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 robust data management practices, supported by relevant policies, procedures, and documentation. Where applicable, this may involve a Joint Controllership Agreement, Data Protection Impact Assessments, Data Sharing Agreements or Memoranda of Understanding, and Service Level Agreements and Charters.

A review of the data requirements of all third-party organisations with access to the PNC or data extracted from it is carried out prior to an organisation being granted access to LEDS data. All organisations are 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.

It is the responsibility of each organisation to ensure that staff members and/or any other person to whom they allow access to LEDS are appropriately vetted and trained to handle and process data in accordance with relevant legislative requirements and the Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) 2023.

11. Sharing and Transferring of Personal Data

Shared access to LEDS data is essential to discharging law enforcement, other policing, national security or safeguarding purposes.

Where it is appropriate, LEDS will be used to facilitate the sharing of data to and from other third-party organisations.

In addition to UK-based organisations, LEDS will be used by law enforcement agencies in the Crown Dependencies: The Bailiwick of Jersey, The Bailiwick of Guernsey, and The Isle of Man. It will also be used by law enforcement in the United Kingdom Overseas Territory, Gibraltar.

The Joint Controllers will ensure that within their police force, in respect of LEDS, international transfers of personal data are compliant with Chapter 5 of Part 3 of the DPA and Chapter V of the UK GDPR.

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.

Any sharing of LEDS data will be underpinned by a documented Data Sharing Agreement or Memorandum of Understanding which sets out the lawful basis for the sharing, along with any legislative purpose limitations and vetting requirements for users of LEDS data.

All Data Sharing Agreements and Memorandum of Understanding will be regularly reviewed.

Any automated disclosure of data outside of LEDS will comply with the logging requirements under Section 62 of the DPA, capturing the date and time of the disclosure and to whom the data has been disclosed. LEDS will also have a mechanism for capturing the reason for the disclosure.

12. Retention and disposal

Each Controller will regularly review and only retain Personal Data for as long as necessary in connection with the purposes it is retained in accordance with Data Protection legislation, and relevant national or local guidelines.

Each Controller is responsible for ensuring the secure destruction or deletion of the Data, in accordance with the requirements of Data Protection legislation as soon as it is no longer necessary to retain it.

For the period of dual running of the PNC and LEDS, data retention will continue to be subject to the PNC RRD rules[7]. Once the PNC has been decommissioned LEDS will have its own Review, Retention and Disposal policy, in accordance with relevant laws and legislation which may be different across multiple jurisdictions.

13. Data Subject Rights

Data Protection legislation establishes rights for data subjects under Chapter 3 of Part 3 of the DPA and Chapter III of the UK GDPR with regard to the processing of their personal data.

Data Subjects are entitled to exercise their rights through any of the Controllers.

The Joint Controllers based in England and Wales, and the NCA, have appointed the 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. ACRO also processes Data Subject Right to Erasure and Right to Rectification requests.

PSNI engages the services of ACRO in relation to Subject Access Requests.

[7] Further details on the specific retention periods for data held within each LEDS Service are documented within the LEDS DPIA 2025.

Police Scotland directly discharges its own responsibilities in relation to Data Subject Rights.

Each Joint Controller and ACRO maintain points of contact within their organisations to facilitate the management of Data Subject Rights, as required by Section 58(3) of the DPA for Law Enforcement Purposes.

Where a Data Subject Rights Request relates to the activities of another Controller(s) (i.e. HMRC, DVLA, DVSA, MIB or a third-party organisation), individuals should exercise their rights directly with that Controller(s). Memoranda of Understanding or Data Sharing Agreements are in place to define and manage the respective responsibilities of each Party in relation to the handling of such requests.

13.1 Complaints

Should a Data Subject have any concerns or complaints in relation to the processing of their personal data, there are established avenues for raising any concerns. Details of how to contact the Controller of their data are set out in individual organisations' Privacy Information Notices. If a Data Subject wishes to raise a concern with the Supervisory Authority about how their personal data has been used, or they believe they have been adversely affected by the handling of their data, they can contact the Information Commissioner who is responsible for ensuring that UK data legislation is complied with, using the information below:

The Information Commissioner's Office
Wycliffe House
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Email: icocasework@ico.org.uk

14. Security

All Controllers are responsible for implementing and maintaining technical and organisational measures to ensure a level of security appropriate to the risk posed by the processing of data in LEDS[8]. The NPCC LEDS Lead keeps such security measures under review.

Robust arrangements are in place to ensure appropriate security of LEDS data, including protection against unauthorised access, unauthorised or unlawful processing and against accidental loss, destruction or damage.

[8] These technical and organisational measures are documented in the LEDS DPIA 2025.

Where risks have been identified to the security and confidentiality of individual's personal data, these have been documented within the LEDS DPIA 2025, and measures have been implemented to eliminate or reduce those risks to an acceptable level before any processing of personal data takes place. Once those procedural and technical solutions have been applied, there are no high risks remaining.

The SSHD as a Processor is subject to Home Office policies, including the Government's Security Policy Framework's (SPF) mandatory requirements, in compliance with other security controls and legislative obligations.

14.1 Security incidents (including data breaches)

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Individual Controllers and Processors of LEDS data have local policies in place for identifying, managing and mitigating any Security Incidents, including a process for reporting data breaches and maintenance of a data breach log. A Security Incident Reporting Guidance for LEDS is also under development.

Data Protection documentation such as Data Processing Contracts, Data Sharing Agreements and a Joint Controllership Agreement are being used to ensure all parties are clear as to their obligations in ensuring the confidentiality of personal data in LEDS and include clauses relating to the reporting of Security Incidents.

Service Level Agreements and Charters will also detail the process for the reporting of Security Incidents for individual organisations that have access to LEDS data.

Risks relating to security incidents and data breaches are set out in the LEDS DPIA 2025 which includes measures to mitigate those risks identified.

The LEDS Security Team is working through the requirements for an ISO 27001, which is the international standard for information security. It shows the necessary steps have been taken to protect data in the event of a breach. Its framework requires organisations to identify information security risks and select appropriate controls to tackle them.

The LEDS Programme achieved the BS 10008 standard for evidential weight and legal admissibility of electronically stored information. This provides strategic assurance that the electronic information in LEDS can withstand legal scrutiny, and that the data being processed is secure, traceable and has not been compromised.

14.2 Vetting Requirements

All system users (police or non-police personnel) must be currently vetted against the appropriate standards in accordance with their data access level as determined by the Vetting Code of Practice 2023, the College of Policing authorised Professional Practice (APP) on Vetting 2024 and the Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) 2023.

Data Sharing Agreements with third-party organisations will include clauses that cover the vetting requirements for users of LEDS data.

15. Governance Framework

Each LEDS controller is responsible for ensuring their organisation complies with any and all obligations arising from the DPA and UK GDPR (or other relevant domestic Data Protection legislation in the case of non-UK-based Controllers).

Several NPCC and Home Office National Governance Boards are being utilised to ensure that the processing of personal data in LEDS is compliant with Data Protection and human rights principles, and that the use of such data is lawful, proportionate and ethical.

All Data Protection compliance documentation is subject to a quality assurance process to ensure that legal requirements are met prior to any processing of personal data.

The College of Policing website provides further information on the Governance and Management of PNC and LEDS.

16. Summary of the evidence to demonstrate compliance with Data Protection responsibilities

Data Protection responsibilities in relation to LEDS are being discharged through a variety of policies and compliance documentation. The table below demonstrates how the development and use of LEDS is being undertaken with Data Protection in mind. These documents are being held on secure Home Office systems.

Policies and compliance documentation	Description
LEDS Data Protection Impact Assessment (DPIA)	A DPIA has been undertaken to help identify and minimise the Data Protection risks at an overarching level. The processing, if not mitigated, could result in a high risk to individuals' rights and freedoms.

	This includes some specified types of processing for specific groups such as children and other vulnerable individuals.
Equality Impact Assessment (EIA)	An EIA is the current method to demonstrate that consideration has been given to the impact of policies and programmes on people who share protected characteristics[9]. An EIA has been undertaken for LEDS and is available on the GOV.UK website.
Child Rights Impact Assessment (CRIA)	A CRIA has been undertaken to focus on how children's rights may be affected by the decisions and actions of governments, institutions and others in the areas of law, policy and practice.
Joint Controllership Agreement (JCA)	A JCA has been agreed by the LEDS Joint Controllers (namely the police forces of England, Wales, Scotland and Northern Ireland, and the National Crime Agency (NCA)) when acting together as Joint Controllers for the processing of Personal Data using the LEDS. It details the arrangements made in compliance with Section 58 of the DPA and Article 26 of the UK GDPR.
Data Processing Contract (DPC)	A DPC has been established between the Joint Controllers and the Home Office to meet the requirement of Section 59 of the DPA 2018 for parties to have in place a binding contract where they have a controller-processor relationship. A DPC has also been established between the Home Office and Amazon Web Services (AWS) as a sub-processor. That agreement sets out the arrangements under which the AWS provides the secure cloud-based platform hosting LEDS.
Data Sharing Agreements (DSAs) / Memoranda of Understanding (MoUs)	Any sharing of LEDS data is underpinned by a DSA or MoU which sets out the lawful basis for the sharing and the responsibilities and obligations of each party.

[9] Defined by Chapter 1 of the Equality Act 2010 as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) 2023.	The aim of this Code is to provide public confidence in the legitimacy and integrity of information that is available through PNC or LEDS and the lawful purposes for which this is applied. It introduced 10 Principles all users must follow, which are underpinned by Data Protection principles. It also provides a framework and operational context for relevant authorities, such as His Majesty's Inspectorate of Constabulary and Fire & Rescue Services to monitor how information within PNC and LEDS is created.
Record of Processing Activities (ROPA)	Data Controllers and the Home Office maintain their own ROPA as required under s61 of the DPA and Article 30 of the UK GDPR.
Privacy Information Notices	Data Controllers are responsible for publishing their own Privacy Information Notice.

Glossary

ACRO – means the ACRO Criminal Records Office established through the National Police Collaboration Agreement relating to the ACRO Criminal Records Office (ACRO) under Section 22a of the Police Act 1996.

Chief Officer – means the Chief Constable or Commissioner of a UK police force and, in the context of the Code of Practice for the Police National Computer (PNC) and Law Enforcement Data Service (LEDS), the Heads of other agencies and organisations connecting to LEDS.

CRIA – means Child Rights Impact Assessment.

Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) – means the Statutory Code issued by the College of Policing, with the approval of the Secretary of State, under section 39A of the Police Act 1996. This Code applies to every chief officer[10] of a police force in England and Wales who has access to LEDS. Every chief officer must have regard to this Code of Practice ('the Code') in discharging any function to which the Code relates[11]. The Code is adopted by other law enforcement agencies, including Police Scotland, Police Service of Northern Ireland and those in other local jurisdictions, and is also applicable to non-police organisations who access LEDS by written agreement.

Competent Authority, Controller, Data Subject, Joint Controller, Law Enforcement Purposes, Personal Data, Processing and Processor have the meanings given to them in the DPA and UK GDPR.

Data Protection Lead – means an individual other than a Joint Controller authorised to act on behalf of the Joint Controllers (the NPCC LEDS Lead acts in this capacity).

Data Protection principles – means Chapter 2 of Part 3 of the DPA and Chapter II of the UK GDPR.

Data Protection Impact Assessment (DPIA) – means an assessment by the Controller carried out in accordance with Articles 35 and 36 of the UK GDPR and sections 64 and 65 of the DPA 2018.

Data Subject Request – means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection legislation relating to their Personal Data.

DPA – means the Data Protection Act 2018.

[10] This Code applies directly to chief officers as defined in section 101 of the Police Act 1996 (as amended).

[11] As required by section 39A(7) of the Police Act 1996.

Erasure or Restriction of Processing Application – means the exercise by a Data Subject of their rights under Section 47 of the DPA, or Article 17 of the UK GDPR and Article 18 of the UK GDPR.

General Processing – means any processing of Personal Data by the Joint Controllers other than for Law Enforcement Purposes.

IAO – means Information Asset Owner.

ICO – means the Information Commissioner's Office; 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. The Data (Use and Access) Act 2025 transfers the functions, staff and assets/liabilities to the new Information Commission. These provisions will not change the role of the regulator; all functions that currently rest with the Information Commissioner will continue to sit with the new Information Commission.

Joint Controllers – means all the Controllers as listed in Appendix A.

Joint Controllership Agreement (JCA) – means the Law Enforcement Data Service (LEDS) Joint Controllership Agreement.

Joint Processing – means any processing of personal data in LEDS (including sensitive processing) by the Joint Controllers.

Lead Controller – means a Joint Controller authorised to act on behalf of the Joint Controllers within the terms of a Joint Controller Agreement.

Lead for Data Subject Rights – means the contact point for Data Subjects as required by Section 58(3) of the DPA for Law Enforcement Purposes.

LEDS DPIA 2025 – means the Data Protection Impact Assessment covering the processing activities of LEDS data, the associated risks and mitigations.

National Agreements – including but not limited to Data Sharing Agreements (DSAs), Memoranda of Understanding (MoUs), Data Processing Contracts (DPCs), Joint Controllership Agreements (JCAs) and Collaboration Agreements where they relate to processing of Personal Data.

NCA – means the National Crime Agency.

NPCC (National Police Chiefs' Council) – means the body formed under Section 22A of the Police Act 1996, consisting of Chief Officers of Police across the United Kingdom, which co-ordinates the work of the police service to protect the public.

NPCC LEDS Lead – means the person nominated to lead on LEDS matters on behalf of the NPCC. The NPCC LEDS Lead fulfils the role of Data Protection Lead for LEDS.

Personal Data Breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data Subject to Joint Controllership.

PS – means Police Scotland.

PSNI – means the Police Service of Northern Ireland.

Security Incident – means an occurrence suspected or confirmed to have led to a compromise of the confidentiality, integrity, or availability of infringement on LEDS. A Personal Data Breach is an example of a Security Incident.

Section 22a Agreement – an agreement is made pursuant to Section 22a of the Police Act 1996 (as amended) which enables police forces, local policing bodies as defined in that Act and other parties as defined in that Act to make an agreement about the discharge of functions by officers and staff, where it is in the interests of the efficiency or effectiveness of their own and other police force areas.

SSHD – the Secretary of State for the Home Department.

Subject Access Request – means the exercise by a Data Subject of their rights under Section 45 of the DPA or Article 15 of the UK GDPR.

SyOPs – means the Security Operating Procedures covering roles and responsibilities, device use and management, etc, which all LEDS users must read, understand and agree to comply with before accessing LEDS.

Technical and Organisational Measures – has the meaning given to it in the DPA and UK GDPR.

UK GDPR – means the United Kingdom General Data Protection Regulation.

Weeding – means a systematic approach to permanently removing unnecessary files from active records.

NB: Any references to a statute or statutory provision, include all subordinate legislation made from time to time under that statute or statutory provision.

Appendix A: LEDS Joint Controllers

The persons and organisations listed below are Joint Controllers as set out in the Law Enforcement Data Service (LEDS) Joint Controllership Agreement (JCA).

(i) The Chief Officers of the following police forces:

Avon & Somerset Constabulary
Bedfordshire Police
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Derbyshire Constabulary
Devon & Cornwall Police
Dorset Police
Durham Constabulary
Dyfed-Powys Police
Essex Police
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
Humberside Police
Kent Police
Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Northern Ireland
Police Service of Scotland
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police

Thames Valley Police
Warwickshire Police
West Mercia Police
West Midlands Police
West Yorkshire Police
Wiltshire Police

ii) The National Crime Agency (NCA)

DOCUMENT END