Introduction to the guidance

Why you should apply the Code of Practice and use this guidance.

First published 31 March 2023 Updated 15 May 2024
10 mins read

PNC and LEDS

This Code of Practice applies to data stored, managed and used through two systems, the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS). Some users will be working entirely through PNC and others will have started the journey towards using LEDS. The principles of the Code apply equally to both systems.

PNC was introduced in 1974. It holds personal data including special category data and other information relating to individuals, including arrests, charges, summons & court disposals (including convictions), warnings and whether a person is wanted or missing as well as information about vehicles and stolen property. PNC data is constituted from data in other systems.

LEDS is a modern cloud-based data service being created to replace PNC. This will provide police forces and other law enforcement agencies with on-demand and joined-up information at their point of need. The full service is expected to be in place by 2026.

The LEDS Programme is working in collaboration with the NPPC, to develop LEDS. The development work on LEDS will then result in the decommissioning of PNC. The LEDS Programme is responsible for delivering the core activities necessary for the transition and for supporting users of the PNC in their undertaking of local activities to deliver this change. The National Police Chiefs Council (NPCC) Operational Communications in Policing (OCiP) team will lead on LEDS Adoption, working with police forces, law enforcement agencies and other partners.

LEDS is being delivered using a product-centric approach with an iterative release of functionality. This means replacing portions of the PNC dataset one at a time in a modular fashion which enables a gradual migration away from PNC for Police Forces and other Law Enforcement organisations. The multiple data sets in PNC are being relocated into LEDS as it emerges. In the interim LEDS is being developed to run in parity with PNC, to ensure the data on both systems is coherent and up

to date. LEDS will eventually become the primary source of law enforcement data rather than PNC. Transactions on the PNC system will be reduced until dependence upon the system is removed entirely, enabling the service to be switched off.

The structure of the LEDS platform will allow the addition of further new data sets in future. For example, Missing and Found Persons capability in LEDS will be a data set specific to LEDS, which evolves once PNC is no longer in use.

Products are simpler to deliver and are designed so that they can evolve rapidly over time. They will be released at different intervals as they mature, and forces are working with the programme to adopt products as they are released, in an order and at a pace that suits them. Non-police organisations are also preparing to on-board.

Core product services

Similar to PNC, LEDS will have 4 core product services.

Person Product

This is the most used product within LEDS and will enable users to search the national person records and update them with the latest person identity information and wanted reports. With the right permissions, persons' records can also be created. This will generally be a user's first port of call, in order to establish whether a person's record exists on LEDS.

The other sub-products are:

- Wanted & Missing Person
- Criminal Justice
- Operational Reports
- Firearms database

Driver Product

This product checks Driver Vehicle Licensing Agency (DVLA) registered Driver Licensing information and will enable Road Policing officers and other investigators of road traffic matters to establish a person's current driving license status, entitlement to drive and other restrictions.

Vehicle Product

This product checks against a vehicle description for information on insurance, tax and police owned reports. LEDS will provide access to DVLA data regarding the vehicle, data on the vehicle's insurance status and on its MoT status.

Property Product

This product will provide the police with a system which allows national reporting and recording of property items, within specified categories, as lost, stolen or found.

LEDS service

These products are supported by LEDS service, which ensure quality, compliance and governance of the data, including;

- Data Quality and Standards
- Auditing
- Alerts and Notifications
- Data Access Processes
- a reporting tool

The 10 principles of the Code of Practice

While the Code itself addresses chief officers, this guidance document aims to provide the whole organisation with supporting information and further direction on how to comply with the ten principles set out in the Code. These are intended to guide those who are responsible for maintaining and securing the integrity of PNC and LEDS as systems, and those using the data and information held within them.

1. Securing the data held on systems

Robust arrangements must be in place to ensure appropriate security of the data, including protection against unauthorised access, unauthorised or unlawful processing and against accidental loss, destruction or damage. This will ensure that the public can have confidence in the integrity and confidentiality of stored information.

2. Creating the data record on PNC or LEDS

Data stored on PNC or LEDS should only be created or entered for law enforcement, other policing or safeguarding purposes. Data records should be adequate, relevant and limited to what is necessary for the specific purpose for which they are being processed. They must conform to the data protection principles and apply national data quality standards. All members of the organisation should understand the importance of high data quality and have access to the necessary tools and support to achieve this.

3. Amending and updating the data record

The data stored on PNC or LEDS must be accurate and up to date. The data will actively be used by agencies who require it to discharge their law enforcement, other policing and safeguarding responsibilities. Legislation requires that the data set is proactively reviewed and updated for accuracy and currency. Any errors that are identified must be rectified as soon as reasonably practicable.

4. Validating the data record

The data available on PNC or LEDS must be correct and relevant. This involves validating or checking the databases to ensure that the information gathered from different data sources is accurate, in a standard format and free of unnecessary duplication.

5. Review, retention and disposal of data

In accordance with the UK data protection regime, data stored and otherwise processed by law enforcement within PNC and LEDS must be regularly reviewed to make informed decisions on retention and deletion of that data, particularly personal data. Data controllers must ensure compliance with all legal and policy requirements to protect the integrity of the data. Where data is in joint controllership, those responsibilities are shared by the joint controllers. Data should be retained for no longer than is necessary. This should follow the formal, national governance process for the review, retention and disposal of data.

6. Accessing and applying the data held

All data held on PNC and LEDS must be processed ethically, professionally and in accordance with the law (including data protection, human rights and equality legislation).

7. Reporting and analysing the data held

Data captured within PNC or LEDS must be assessed for accuracy and carefully analysed, so that the results are reliable to guide decision making and/or resource allocation.

????????8. Sharing data that is held

Shared access to data is essential to discharging law enforcement, other policing, national security or safeguarding purposes. The Code seeks to encourage effective data disclosure to better support law enforcement and public protection. This should always conform to requirements of the law, as well as ethical and professional standards.

????????9. Accountability for and auditing of data access and usage

Data protection legislation places obligations on controllers to demonstrate their compliance by putting into place appropriate and effective data protection measures. This includes measures such as local auditing of access and processing activity.

????????10. Training and continuing professional development

Regular training and learning will ensure system integrity, better protection of data subjects' rights and better outcomes for law enforcement. Arrangements must be in place within all user organisations to train new users and proactively support continuing professional development, to ensure that the highest levels of data literacy are achieved and maintained.

Structure of the guidance

The guidance is relevant to all organisations that are granted access to PNC and LEDS, the managers, members and staff of these organisations, and suppliers, auditors and trainers who hold responsibilities to support those principles and understand whether they have been met.

The Code and the guidance taken together provide the ‘what’ to do, with other existing documents referenced as existing practice guidance. Further documents will be created to elaborate on the ‘how’.

The Code of Practice for PNC published in 2005 is now considered out of date and was withdrawn when the new Code was approved by Parliament. The new joint Code of Practice for both PNC and LEDS will now take effect until PNC has been decommissioned. Some lead-in time will be allowed to enable organisations to ensure that they are compliant with the new provisions. The 2005 Code only relates to police business processes that require interaction with the PNC Names database for the purposes of recording the commencement and conclusion of process relating to recordable offences. The 2023 Code covers all aspects of PNC access, as well as the transition towards full use of LEDS.

Training

A comprehensive training programme is in place for PNC, and learning for the practical application of LEDS products has also been produced through LEDS Adoption.

Further mandatory learning for continuing professional development – the PNC and LEDS Code of Practice Learning Programme – has been developed to provide support to enable forces and other users to comply with the principles and responsibilities within the Code and guidance document.

The first four mandatory modules were launched in January 2024, with three specialist modules; Security, Audit and Data Creation, to follow in Spring 2024.

Other supporting guidance

PNC has an extensive user manual and set of business rules, which will be maintained until PNC is decommissioned.

Some guidance for each of the LEDS products will be published at first technical launch and will be refreshed as the iterative development of the system progresses. For LEDS, a set of specific guidance documents for each product will be created, together with some overarching guidance on common themes.

To support implementation of the Code of Practice an implementation framework tool has been developed by OCiP. A working group of PNC specialists from across forces and some non-police organisations have created the tool to support police forces and other PNC and LEDS users, in demonstrating their compliance with the Code of Practice. This offers an opportunity to review current procedures in data security, data management and data application using PNC and, where appropriate LEDS, to meet the new guidelines and ensure that good practice is in place.

The tool is presented as a **self-assessment Word template to be used by forces** (available on Knowledge Hub for members of the LEDS group) to assess current levels of compliance and plan for remedial action if that is required. Those forces and other organisations that are preparing to adopt LEDS products can use this as part of local implementation plans and ensure they are compliant ahead of signing up. An example version has been created with examples of suggested evidence put forward by the working group and there is a simple guide to use.

This will also address deficits in readiness for compliance with the Code to be reviewed prior to any future inspection process. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) were represented on the working group to provide feedback on the usefulness of the proposed tool for general inspection purposes. Compliance with the statutory Code may now be considered within general inspection of forces, although there are no immediate plans for any specific thematic reviews. HMICFRS will consider a completed self-assessment as evidence towards compliance.

Knowledge Hub

Further information on LEDS product development is available through **Knowledge Hub (you will need to log in)**.

This is a closed group for those who work in or with local or national policing. Registration is free but membership requests will be subject to approval. General enquiries can be directed to **LEDS@homeoffice.gov.uk**.

Authorised professional practice

This guidance also contain references to authorised professional practice (APP), which is practice guidance for policing, issued by the professional body, the College of Policing. This is generally open to other organisations who use PNC and LEDS, who may wish to use this to inform their

internal practice guidance, where relevant.

Performance measures

There will also be some performance measures for both PNC and LEDS. The performance measures may include training, data quality measures, operational-critical measures such as timeliness of data entry, data security and supplier requirements. For example, there were specified timeliness targets in the 2005 Code for PNC, which have been reconsidered and refreshed and are still endorsed by the NPCC.

Further measures will be developed by subject matter experts working under the governance of the NPCC lead for PNC and LEDS. They will be based on existing standards and targets (such as the two for PNC timeliness), as well as identifying or developing additional measures that are required for operational efficiency. Particular attention is being paid to promoting improvements in data quality, using the six data-quality dimensions, which form the **data quality standards**.

Tags

Information management