Governance and management of PNC and LEDS

How the systems are being governed.

First published 31 March 2023

10 mins read

Governance structures

For the purposes of the Code, the Home Office and the NPCC hold responsibilities in relation to the operation of both PNC and LEDS, as well as in providing leadership and direction to the law enforcement agencies that access the data within the systems. Organisations accessing the systems will be required to ensure that managers and users of the systems are fully supported to undertake appropriate training, learning and development for the use of the platforms and data and to remain updated. More information will be published in 2022 as to the mechanisms through which this will be supported, as part of the wider adoption support.

NPCC

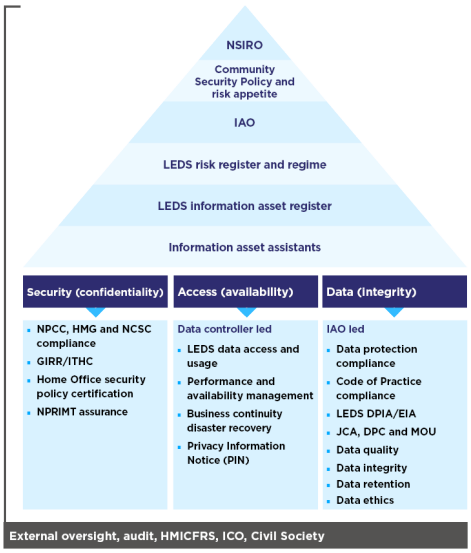
There is a set of NPCC-led structures that have historically supported PNC governance steered by the NPCC and overseen by what is now known as the Digital, Data and Technology Coordination Committee (DDaTCC). This is led by the NPCC lead for Digital, Data and Technology, who also acts as the national senior information risk owner (NSIRO) on behalf of the joint controllers (see **data protection roles**). The NPCC has created a National Police Data Office (NPDO) and National Police Data Board (NPDB) to deliver the National Policing Digital Strategy 2020-2030. These bodies will look to continue and strengthen a lot of the work that has been undertaken to facilitate data-driven policing and will support LEDS and other data programmes. The NPDB brings together subject matter experts in relation to data quality, records management, data protection and data sharing, the aim being to create a consistent framework for the management and use of data.

Evolving governance for PNC/LEDS

As of February 2023, the governance structures for LEDS as a system are still evolving. During transition all of the key elements that are in place for PNC governance will be continued but as

LEDS is developing, a new overarching governance structure is being determined, which reflects the different architecture of the system, and long term sustainability demands. Existing PNC governance arrangements build upon data protection compliance structures and the former Code of Practice for PNC (2005).

The initial LEDS governance structure will run in parallel with the existing PNC governance model while LEDS gradually takes over PNC functions. This reinforces compliance with data protection legislation by implementing the governance responsibilities identified in that legislation as well as wider security and data quality considerations. As well as the data protection role of NSIRO there is an NPCC-appointed Information Asset Owner (IAO) who also oversees compliance for both systems.



The LEDS programme will continue to be managed by the Home Office as a delivery agent that supports both system build and sustainment structure until LEDS is fully established. The LEDS Adoption Team will work with the IAO to enable forces to prepare for adoption during the longer-term transition from PNC to LEDS.

Applications for access

All applications for access to PNC are subject to a transparent approval process. This process is governed by the Police Information Access Panel (PIAP), led by the IAO on behalf of the joint controllers (**read more information on joint-controller relationships**). This process will include applications from commercial organisations to allow them limited access to redacted or filtered data

for use in applications that support law enforcement purposes, such as checking for vehicle fraud. PIAP is also overseeing access to LEDS, whilst that is in development.

Information assurance and security

Principle 1 of the Code is **Securing the data held on systems**. This places responsibilities on chief officers, both as joint-controllers of the national systems and as controllers of their local systems, to ensure that there are robust arrangements in place to ensure appropriate security of the data.

This is also known as Information Assurance (IA), the processes which safeguard the confidentiality, integrity and availability of data used by individuals or organisations. This involves

- managing the risks associated with creating, using, processing, storing, transferring and deleting data.
- preserving confidentiality of information involves restricting access to personal or operational information, including defending against external threats
- protecting the integrity of information entails guarding against unauthorised alteration or destruction of data and the accuracy and provenance of data – for example, do we trust the source of this data, is it correct?

Finally, maintaining the availability of information systems requires ensuring that access to information by users or systems is authorised, reliable and timely.

At a national level security governance for both PNC and LEDS is provided by:

- the NSIRO – the national policing lead for DDaTCC is NSIRO for both systems
- the Police Information Assurance Board (PIAB) – which provides the strategic lead on the development, implementation and evaluation of IA within national policing
- the IAO – also a role shared across both systems
- national information risk assurers
- a Security Working Group which is evolving the longer term security governance for LEDS

Responsibilities

These arrangements will be replicated locally in individual forces and other agencies which might contribute data to PNC or LEDS.

The NSIRO is responsible for information risk associated with the national capability, and police force/or other agencies appoint senior information risk owners (SIROs) responsible for information risk within their organisations. Likewise there will be local IAOs.

An information security officer (ISO) responsible for the development and implementation of information security policies and procedures within their force/agency. The ISO may also be responsible for information assurance, or there may be a separate information risk assurer role.

These positions maintain the assurance and security of data in local police systems. Further detail on roles and responsibilities in relation to information assurance is outlined in the **College of Policing APP on Information Assurance**.

Risk assurance

As a national police information system both PNC and LEDS are continually assessed for compliance to the **NPCC's National Policing Community Security Policy** and the National Policing Information Risk Assurance Policy to ensure that each system is managed within the 'Cautious' risk appetite described in the **NPCC National Information Risk Appetite Statement**.

To meet the needs of law enforcement and public safety outcomes, the systems should be compliant with **HMG Security Policy Framework** and follow the guidance of the **National Cyber Security Centre (NCSC)**. This is supported by the Police Cyber Assurance Framework managed by the **Police Digital Service** (PDS).

PDS will work with police forces to review whether their own supply systems are fit for purpose. They will also review the implications of contractual relationships with vendors of those systems and ensure their compliance with the National Policing Information Risk Assurance Policy.

Chief officers and chief executive officers who use PNC and LEDS are required to provide an annual assessment of how their internal systems are working and how their suppliers are meeting obligations.

Code of Connection

As part of the access arrangements for both PNC and LEDS there are written agreements which stipulate the technical and security conditions that must be in place and maintained to facilitate access to the systems. The Code of Connection (CoCo) for each system will be issued on behalf of the IAO. This is based on a threat/risk assessment and agreement of the required controls to treat risks. This employs the three tests of confidentiality, integrity and availability.

Each CoCo will also include:

- the ongoing requirements, both technical and procedural
- the need to audit to national standards
- the recertification process
- how data breaches should be pre-empted
- if necessary, how breaches should be managed and reported

For LEDS this will also outline the requirement for connecting organisations to use the **National Identity Access Management (NIAM) broker**. Given that the threat / risk assessments for systems that connect to LEDS may differ (depending on the system consuming LEDS data) there may be several CoCo's in operation. for example, Police Forces via NIAM, SRG applications (Standard interface Replacement Gateway) or other Law Enforcement Agencies (LEA) connecting to LEDS.

Below the organisational level of the CoCo there is a further level of security compliance at a product level, Security Operating Procedures (SyOps) Where the CoCo is more system-led, the SyOps provide more guidance on how operational users should be managed and what the requirements of security compliance at that level. This will include the relevant vetting levels for each product (**see Vetting**).

Suppliers of services to these connecting organisations will also be subject to data-processing contracts that set out their contractual responsibilities under the respective Code of Connection. These include:

- complying with data protection legislation
- adhering to the expectations of the Code
- ensuring that any systems connecting with the platform align with current requirements
- producing timetabled remedial plans where a supplier's product is not compliant with the Code, guidance document, performance metrics or any defined business rules
- assist inspections at any time to ensure compliance

Vetting

Principle 1 of the Code creates a responsibility on chief officers to confirm that people who are granted access to either or both the systems are appropriately vetted on appointment, or upon transfer into a role where this becomes necessary. All PNC users are required to hold the necessary vetting in order to be permitted access to PNC data. All vetting authorities will be monitored as part of the HMICFRS/HO audit process.

The vetting standards for the police service are determined by the **Vetting Code of Practice 2023** and College of Policing **authorised professional practice (APP) on Vetting**. There are two vetting regimes in the police service:

- force vetting – designed to protect police assets
- national security vetting (NSV) – designed to protect government assets

There is some commonality between the threats posed to police assets and government assets, but there are differences. The two regimes, therefore, have different decision-making criteria and the vetting enquiries involved draw on distinct information sources. Force vetting levels are applied to all individuals who require unsupervised access to police assets (including information, systems or premises). Some of these individuals also require access to government security classified (GSC) information and, where this is the case, the appropriate level of NSV is applied.

There are three levels of force vetting applicable to the police service:

- recruitment vetting (RV)
- management vetting (MV)
- non-police personnel vetting (NPPV)

Vetting Standards for PNC

All Police and police staff PNC users are required to hold at least Recruitment Vetting (RV) level security vetting to access PNC.

Access levels	Vetting level

Direct PNC Access – Enquiry	RV/NPPV L2
Direct PNC Access – Enquiry & Update	RV/NPPV L2

The vetting standards for non-police organisations are achieved through applying the relevant NPPV or NSV levels. NSV is also the regime that applies to any individuals working with or on behalf of a government department.

Vetting Levels for LEDS

The vetting requirement is underpinned by the connecting systems which will stipulate that as a prerequisite for access, all staff and contractors within policing and non-police law enforcement or safeguarding agencies will be required to have an appropriate level of vetting in place, in accordance with the relevant SyOps. This will also be determined in accordance with their data access level.

National Identity and Access Management tool (NIAM)

LEDS utilises NIAM as the authentication/authorisation broker for individual user access. A LEDS user from a connecting force will access LEDS products via the NIAM connection. Once a user requests access to a LEDS application, NIAM will pass the authentication/authorisation request onto the forces own identity provider, for example, Azure AD, to authenticate the user and their entitlement before the user is authorised to perform against that application. NIAM will return this information to LEDS to confirm access is allowed. This replaces the password system used by PNC.

NIAM is already used by some other criminal justice systems, as well as LEDS. For a police force or other law enforcement organisation to access a NIAM protected application, the relevant force or organisation, will need to be registered and on boarded, for example the LEDS Property application is registered in NIAM so the force needs to be onboarded to NIAM to access LEDS Property. A requirement for organisations is that they have adequate business change, security and other controls in place as part of local assurance to check whether a user's roles and entitlements are still required. The NIAM Code of Connection for LEDS stipulates such requirements.

Tags

Information management