Governance and management of PNC and LEDS

How the systems are being governed.

First published 31 March 2023 Updated 15 May 2024
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.

A package of continuing professional development for current PNC and LEDS users is now **available on College Learn** (you will need to log in). New users of LEDS products are supported with guidance as part of the wider adoption support of the LEDS programme.

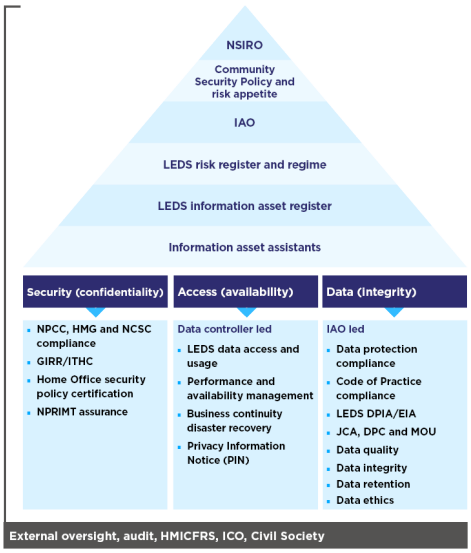
NPCC

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 through national and local systems.

Evolving governance for PNC/LEDS

As of January 2024, the governance structures for LEDS as a system are still evolving. Whilst PNC and LEDS are operating in parity 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 and other user organisations 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), which is made up of a cross-section of expertise who meet to consider each applicant for access, led by the IAO on behalf of the joint controllers. PIAP considers applications for access to the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS), including any requests for downloads and data extracts. PIAP will also consider requests for systems which access PNC/LEDS information through interfacing systems, downloads, or extracts their data, such as the Violent and Sex Offenders Register (ViSOR) and the National Firearms Licensing Management System (NFLMS), to ensure there is not a negative impact on the service.

This 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, such as checking for vehicle fraud.

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**.

A specific security module is being developed by the College of Policing as part of the continuing professional development package, this will be made available in early spring 2024. This identifies the responsibilities each user organisation has in regard to the security of PNC and LEDS and the data contained within them.

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 and the **National Information Risk Management Framework (you will need to log in to Knowledge Hub)**.

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).

The National Police Information Risk Management Team (NPIRMT) role has now transferred to the PDS on behalf of National Policing. PDS Cyber Security has now taken on the role of providing assurance services to Police and Public Protection Technology programmes by using the Secure by Design Assurance Framework.

Standards certification

The LEDS programme is currently working towards attainment of BS10008 Certification for Evidential Weight and Legal Admissibility of Electronically Stored Information. This is an internationally recognised standard which will enable Police Forces and other law enforcement organisations to present data obtained from LEDS data into court with confidence that it has evidential weight.

The standard aims to ensure information stored in computer systems is trustworthy. That is, the information can be confidently used to make decisions and/or be presented in Court as evidence or supporting evidence.

Law enforcement colleagues who access data from LEDS will able to rebut challenges to the authenticity and integrity of the information LEDS Products hold. They should be able to demonstrate in Court that LEDS as a system is reliable and can be trusted.

Certification by BSI is done in two stages. An initial audit process has reviewed the policies, solution documentation and procedures that are in place for LEDS as it is being developed to make sure they comply with the requirements of the standard. A second stage audit will later make sure policies, solution documentation and procedures are implemented and adhered to and allowing the British Standards Institute to issue a certificate.

The LEDS Security Team are also implementing ISO/IEC 27001. ISO is the International Standards Organisation and this is therefore an internationally recognised standard. This certification recognises that an organisation has put in place systems to manage risks related to security of data owned or processed by the organisation. These systems are described below. This also links to the

UK Government Secure by Design Process.

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.

Technical and security conditions

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. A Code of Connection (CoCo) may 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.

There is one in place for PNC, but at present LEDS has not developed a LEDS-specific CoCo as assurance is given via NIAM. 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. The programme may create a LEDS CoCo for those entities that are not connecting via an assured means, that is, through NIAM.

A 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

National Identity and Access Management tool (NIAM)

The National Identity Access Management (NIAM) solution is the assured, recommended methodology for all national applications to be consumed from. All police forces have been assured to connect to NIAM and to access data, other policing partner agencies or, non-policing authorities will need to be onboarded.

LEDS utilises NIAM as the authentication token holder for all forces, as the National Identity Access Management provider. LEDS is delivered via Entitlements that contain different functionality. LEDS Entitlements should be assigned via an Identity Access Management application based on the job function of the person. It is important to understand with every request made for a user to be granted access that internally a review is done to understand exactly what functionality might they require.

Access granted should be proportionate and relevant to their job function within the force or agency. No user should be given access to functionality that they do not have a legitimate purpose for using.

When a LEDS user from a NIAM connected organisation attempts to access LEDS, NIAM will pass the authentication or authorisation request onto the organisation’s own identity provider, for example, SailPoint, to authenticate the user and their entitlements, 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. This process follows the directions set out in the PDS Blueprint that all forces and other connecting organisations should adhere to and that PDS assurances are provided against.

A risk rating or security score is assigned by PDS to each force or organisation requesting access to LEDS. This is measured against the NIST matrix, which provides a maturity score against that

force or non-policing organisations' security position.

NIAM apply two processes that provide assurance for connecting organisations:

1. SyAP – The SyAP Tool (Security Assessment for Policing), is the means for assessing the security maturity of core policing organisations.
2. TPAP – Third Party Assurance for Policing (TPAP) process which is to ensure policing has sufficient assurance with their suppliers of services, partners, and contractors.

Below the organisational level 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**).

Further guidance is currently being produced with regard to security requirements for access to either system either working from home, or remotely from another location, including overseas. In recent years there has been an increase in hybrid working and as a web-based system, LEDS is intended to be more accessible to users who are not at a fixed terminal.

Additional caution is required when working with information in a non-secure setting. It is important that mobile data systems are kept securely and that, in the same way that you would at work, you prevent people from being able to see your screen by not working with your screen facing windows and areas where you can be easily overlooked. Using privacy screens on monitors or the in-built ones on laptops can also assist in keeping information secure.

Specific guidance may also be in place regarding homeworking, for example, in 2020 a PNC Liaison Officer Letter was submitted stating that anyone who was part of the **Homes for Ukraine scheme** must not access PNC and PND from home. This is still in place at the time of writing as is similar guidance regarding hosting refugees from Afghanistan.

Further guidance for users accessing overseas is available in the NPCC approved 'Overseas IT Access Guidelines'. As with other documents in National Cyber Policy & Standards, access to this document is limited to members of the Community Security Policy Framework.

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

- complying with data protection legislation
- adhering to the expectations of the Code of Practice
- 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 expected security requirements, guidance document, performance metrics or any defined business rules
- assist inspections at any time to ensure compliance

Security Incidents

A Security Incident may be defined as “an unwanted event that could endanger the confidentiality, integrity, or availability of information’.

Examples include (but are not limited to):

- leaving information out on desks or printers
- failing to lock a screen or laptop when away from a workstation
- failing to keep a system password or PIN safe, or allowing others to use either of them
- deliberate or accidental corruption of data
- unauthorised access to a secure computer system
- unauthorised disclosure of information

Security incident describes an event where security policies and procedures have not been followed so security being violated. Breach includes a compromise to data, where there is unauthorised access to data. This includes incidents that do not impact on the data, for example, a laptop is lost but no one gains access to the data.

The examples listed above also constitute a breach as they involve business or personal data (or information). Some of that data may relate to policies and processes or otherwise sensitive materials which could impact on public safety or national security if compromised. A breach is any event which has resulted or may result in:

- unauthorised access to data
- unauthorised disclosure of data
- loss of access to data
- loss of data integrity, including accuracy

A specific type of data is personal data, which is covered in further detail below. A breach could involve both personal and non-personal data.

Personal?data breach

Data protection legislation [Article 4(12) UK?GDPR and section 33(3) DPA] defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

There will be a personal data breach whenever:

- any personal data is lost, destroyed, corrupted or wrongfully disclosed
- someone accesses personal data or passes it on without proper authorisation
- personal data is made unavailable, for example, when it has been encrypted by ransomware, or is accidentally lost or destroyed

Examples of personal data breaches include:

- access by an unauthorised third party
- sending personal data to an incorrect recipient

Reporting Security Incidents

Forces and agencies are expected to have their own local security incident procedures that include deciding whether the incident is likely to have immediate or serious repercussions for the rest of the community.

Where an incident is assessed as having only local impact, it should be dealt with following the local procedure, and then reported to the National Management Centre (NMC), managed by PDS, as part of the regular return of security incidents.

Local reports are used to monitor and report on current threats or incidents faced by the policing community. The information is incorporated into the national policing information threat model. It includes the frequency, future likelihood of occurrence and any specific impacts this would have on national policing.

Forces and agencies are required to report fast-time security incidents that may affect other members of the policing community to the NMC Cyber Intelligence and Threat Manager. Appropriate action can then be taken to prevent widespread confidentiality, integrity or availability issues occurring. This information is also used to monitor and report on current threats to the police service and feeds into the national policing information threat model.

A personal data breach is unauthorised access to person or sensitive data. This is the type of breach that is reported to the ICO.

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**
- College of Policing **authorised professional practice (APP) on Vetting**
- **NPCC PDS Vetting Requirements for Policing Standard** which provides specific advice on vetting for access to police data systems

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.

Type of access	Vetting level
Direct PNC access – full enquiry and full update	NPPV level 3
Direct PNC access – full enquiry and restricted update (can only update certain parts of a names record	NPPV level 3
Direct PNC access – enquiry only	NPPV level 2
Names download – personalised	NPPV level 2

Type of access	Vetting level
Names download – de-personalised	BPSS
Plant download – de-personalised	BPSS
Stolen vehicles download – de-personalised	BPSS
Stolen firearms download – de-personalised	BPSS

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 entitlement.

Tags

Information management