Principles

This section of the guidance underpins the 10 principles for the professional and ethical use of PNC and LEDS, which are set out in the Code

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

Introduction to the ten principles

This section of the guidance explains the 10 principles for the professional and ethical use of PNC and LEDS.

It supports the Code by providing details on the reasoning behind the principles, as well as what responsibilities and actions support each one. PNC and LEDS users are expected to read the whole Code but can use this guidance to gain insight into the most relevant principles.

These principles are relevant to:

- all organisations that are granted access to PNC and LEDS
- the managers, members and staff of these organisations
- suppliers, auditors and trainers

Layout of the principles

In this section there is a short overview that:

- identifies each of the 10 principles within the Code
- explains the overall requirements that support that principle and the related data function
- signposts references to specific guidance or legislation that should be read

Responsibilities at each level

The overview is then followed by a description of the responsibilities or obligations that follow at each level, which include responsibilities under data protection legislation.

Chief officers

The chief officer is the head of the of the organisation that has access to PNC and LEDS. The Code applies directly to specific chief officers of police. Chief officers of other police forces or other agencies and organisations who have been granted access to PNC and LEDS by written agreement will also be required to follow the Code, so the term chief officer applies to all heads of connecting organisations.

Operational managers

Operational managers within the organisations are managers who at any level will have some responsibility for:

- managing the operation of PNC and LEDS within that organisation
- the performance of personnel who may be granted access to the platform

Not all the responsibilities outlined will be ascribed to one individual management role. There are different individuals operating at relevant levels who will assume these responsibilities, acting on behalf of the organisation.

System users

A system user is an individual who has been vetted and approved to use PNC and LEDS and trained in the functionality. They will either be registered to log in as a direct user or vetted and approved for access through a connecting system.

A systems user may:

- have a role with a specific data function – for example, data entry
- be using information from the systems as part of a wider law enforcement or safeguarding role – for example, a frontline police officer accessing information for operational reasons

NPCC

The NPCC acts as a coordinating body for police forces across the United Kingdom and has a role in providing leadership and direction to police forces who use PNC and LEDS.

This guidance sets out NPCC's responsibilities to strategic oversight of both systems on behalf of policing. This is in accordance with their legal position representing the joint controllers of the systems and their operational oversight of police, in the access to and application of data through the systems.

Non-police bodies are expected to follow the same policy and practice.

Home Office

The Home Office currently hosts the programme that is developing the LEDS platform, as well as some ongoing technical management of the PNC structure. The Home Office responsibilities for LEDS may be adopted by a new sustainment body in the coming years.

The Home Office does not have statutory responsibility for many of the bodies accessing the systems. This guidance sets out the responsibilities in relation to its role in the governance and management of the infrastructure of the systems (rather than the content of those systems). This is distinct from the Home Office role as a processor on behalf of the controllers of the systems through various departments.

Other bodies

Other bodies may also be referenced in respect of their relationships and responsibilities in supporting PNC and LEDS. These include the:

- College of Policing
- Police Digital Service

The responsibilities set out under each principle will be relevant to that specific data function but there may be some overlaps between sections.

For example, it is repeated across data functions that people who access both PNC and LEDS are:

- vetted
- fully trained (in accordance with the national learning strategy and agreed national standards)
- up to date with current practice guidance
- fully understand all requirements and responsibilities

Further suggested guidance

There are references to suggested additional guidance on expected performance and practice for each principle.

The College of Policing produces authorised professional practice (APP) and other guidance that support expectations of good practice.

His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) will apply the same standards to all organisations. They will use the Code and this guidance, together with the suggested further guidance, as the benchmark of expected practice. While written to support policing, other law enforcement agencies should access APP and incorporate it into their own context. Police Scotland, PSNI and other local policing jurisdictions may have their own localised guidance. It is recommended that all PNC and LEDs users consider this additional guidance.

1. Securing the data held on systems

Principle

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.

Requirement

Law enforcement is an increasingly information-led activity. Maintaining security requires robust information assurance structures and processes. Assuring security is also reliant on the technical functionality of the systems that exchange information with both PNC and LEDS.

The UK GDPR and Part 3 of the DPA 2018 introduce a duty on all law enforcement organisations to report personal data breaches to the Information Commissioner's Office (ICO) without delay if there is a likely risk to the rights and freedoms of individuals. Personal data breaches have potential for heavy financial penalty.

The sixth data protection principle of Part 3 of the DPA 2018 is that personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

A National Senior Information Risk Owner (NSIRO) is appointed by the NPCC to act on behalf of the joint controllers for both systems, and to oversee and manage risks to the systems. In turn,

each organisation that connects with PNC and LEDS will be liable through its chief officer (or equivalent) for the efficiency and security of their systems, their suppliers and the personnel who access and use the data, either directly or indirectly.

This responsibility for data security may be delegated to a named senior individual, the senior information risk owner (SIRO), who is familiar with information risks and management of information risk. The SIRO may, in turn, be supported by an information asset owner (IAO) and information security officer (ISO). Police forces are required to designate a data protection officer (DPO) for general processing (as police forces are ‘public authorities’), and the same for law enforcement processing (as they are ‘competent authorities’).

Primary responsibility for organisational and user compliance with the Code and legislation remains with chief officers (and equivalents in other organisations).

Why is this relevant?

Data on PNC and LEDS will be drawn from a range of sources. These include local and national records of crime, reports of missing people, and details of convicted sexual and violent offenders. LEDS will also provide an interface for access with other databases, such as the Driver and Vehicle Licensing Agency (DVLA) for driver and vehicle records.

Different data systems are used by forces and other law enforcement agencies to house data sources that will connect with PNC and LEDS.

Any compromise to data security could lead to:

- the facilitation of crime
- issues of public safety
- hindrance to investigations
- financial loss
- damage to individuals whose information is held
- damage to the reputations of joint controllers, the NPCC and other stakeholders such as the Home Office as technical systems manager

The Home Office, as technical systems manager on behalf of the joint controllers for both PNC or LEDS, will provide details of the specific technical and procedural systems requirements.

Access agreements to PNC and LEDS will include conditions to provide assurance of compliance. The conditions will include that:

- access to information on PNC or LEDS is restricted to organisations that have an identifiable lawful purpose
- personnel who access PNC and/or LEDS within both police and non-police organisations are appropriately vetted and managed
- individual access to information is proportionate to what is required in discharging a lawful purpose
- requirements for maintaining data security and the penalties for any organisational breaches of data security are clearly stipulated

Further suggested guidance

- **APP on information assurance**
- **Vetting Code of Practice**
- **The ICO Guide to Law Enforcement Processing**

For police services only

- National policing Community Security Policy (CSP) National Policing Information Risk Assurance Policy.

What do you need to do to meet this requirement?

Chief officers

As a chief officer, you will be responsible for:

- ensuring that the DPA 2018 and UK GDPR are adhered to in managing connection to PNC or LEDS
- nominating a senior individual to act as Information Asset Owner for the data, who should provide assurance regarding information risks to the SIRO – together with the DPO, they are responsible for providing expertise and advice to assist the relevant data controller
- procuring and maintaining systems that can provide the appropriate technical and security assurance to connect to either PNC or LEDS

- providing information and technical assurance about the security of data systems through required assurance frameworks, such as those managed by the Police Digital Service
- maintaining security of all local assets that are used to access PNC or LEDS
- ensuring that the information risk is recorded and that appropriate risk management processes are in place
- confirming that people who are granted access or entitlement to either or both these systems are appropriately vetted on appointment, or upon transfer into a role where this becomes necessary
- ensuring that access is removed upon the individual leaving the organisation, transferring to a role that no longer warrants access or is subject to disciplinary or criminal processes
- ensuring that there is an audit trail for each local access event, including measure to satisfy s62 DPA 2018, as well as clear audit capability and processes to support maintenance of data security

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that people who access PNC or LEDS are fully trained in accordance with the national learning strategy and agreed national standards, are up to date with current practice guidance, and fully understand all requirements and responsibilities in accessing the platform
- monitoring the work of those who access data to ensure that entitlement is restricted by role and by relevant purpose

Systems users

As a systems user, you are responsible for:

- using data access controls responsibly – this includes not sharing passwords or recording passwords in ways that could be compromised, and not viewing PNC or LEDS through another person’s permitted access
- exercising caution in printing and exporting data from the database as hard-copy data may quickly become out of date or inaccurate and will need to be disposed or stored securely, referencing the source, date and purpose for extraction
- anonymising extracted information if it is not necessary to identify personal details
- maintaining personal levels of integrity, to the standard that exists for policing through the Code of Ethics, or equivalent

- reporting any changes in personal circumstances that may affect security clearance or may cause a compromise of integrity, following the guidance issued by the **College of Policing Vetting Code of Practice**
- reporting any suspicious or unusual activity that might suggest malpractice on the part of others
- keeping personal knowledge of security requirements up to date by becoming familiar with the Code, proactively checking for system and legislation updates, reading technical guidance and seeking advice when required

NPCC

The NPCC will support chief officers by:

- appointing (on behalf of the joint controllers collectively) a NSIRO with responsibility for ensuring that both national systems are appropriately risk assessed, and that risks are monitored and managed in accordance with the National Policing Information Risk Assurance Policy
- ensuring that where relevant or required clearly defined joint-controller agreements, memoranda of understanding and data-processing agreements have been put in place between and on behalf of the joint controllers
- providing leadership and operational advice to police forces, to ensure that maintaining security and integrity of data is a high priority for all platform users
- working with the College of Policing to ensure that policy and guidance reflect current legislation and regulatory requirements, and that any changes are communicated to the relevant organisations in a timely manner
- working through the Police Digital Service to apply assurance controls which ensure that systems that will exchange information with PNC and LEDS meet the desired information security and assurance requirements

Home Office

The Home Office will support chief officers by ensuring that the platform has in-built restrictions to prevent:

- unauthorised use of PNC or LEDS
- unauthorised use of specific data sets within the systems

2. Creating the data record

Principle

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 minimum 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.

Requirement

For information to be valid and informative, its structure and meaning need to be understood by all parties intending to use or handle it.

Law enforcement agencies may be liable for action in response to judgements made upon the data contained within the information, so it is essential that there is confidence in the accuracy and currency of that data. It is expected that those organisations entering or uploading data onto PNC or LEDS will comply with law enforcement **POLE (Person, Object, Location, Event)** data standards for creating data entries and **core data quality dimensions** for the public sector.

All personal data created or processed within PNC or LEDS is subject to the relevant provisions of the DPA 2018 and the UK GDPR, as appropriate.

For example, under the fourth data protection principle of the DPA 2018, there is a need to be able to distinguish, as far as possible, between personal data that is based on factual data and that which is based on a personal assessment, such as a witness statement.

Individuals have the right to be informed about the processing of their personal data and need to have confidence in the accuracy and currency of any data held. A privacy notice on the organisation’s website should therefore be supplemented by supporting information for the public as to how personal data records can be accessed.

Why is this relevant?

Data on PNC or LEDS may be uploaded by bulk transfer, or a record may be created or amended by an individual acting on behalf of a police service or other law enforcement agency.

Having information on a single accessible data source allows that information to be shared among agencies who require it to discharge their law enforcement, other policing or safeguarding responsibilities. Such agencies range from statutory local and national bodies – for example, government departments – to bodies such as the Child and Family Court Advisory and Support Service. This will widen with the inclusion of a LEDS product for Missing Person. Agencies must be confident that the data is fit for purpose, of high quality and integrity, and suitable to be admitted to a court of law when applicable.

In the context of law enforcement data, quality and clarity are imperative, as there are implications and risks in creating an inaccurate or incomprehensible data record. High-quality data will support and inform a decision-making process that is auditable, transparent and capable of being corroborated with other related information. High-quality data will also ensure that the risk that a person presents, or the risk that a person may be subjected to, is fully understood.

Further suggested guidance

- **The Information Commissioner's Office Guide to Law Enforcement Processing**
- **APP on information management**
- **APP on data protection**
- **ACPO PNC Compliance Strategy (2000)**
- **The Home Office HMIC Report Police National Computer Data Quality and Timeliness (2001)**

For police services only

Force Data Protection Officers can access the NPCC Data Protection Manual of Guidance.

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- confirming that any personal data is processed in line with the data protection legislation, and that the personal data is adequate, relevant and not excessive in relation to the purpose for which it is processed
- ensuring that any personal data is collected for specified, explicit and lawful purposes, and not further processed in a manner that is incompatible with those purposes
- ensuring that the work of those who enter and maintain data is carried out in line with national minimum data quality standards
- ensuring that there is a systematic process for conducting regular quality checks, to confirm that all data is entered in accordance with national minimum data quality standards and that the results of data quality monitoring are collated and reported
- ensuring that regularly updated guidance on data quality is disseminated to relevant managers and staff within the organisation, to ensure that practice remains valid in line with current national guidelines and legal obligations
- ensuring that data is entered onto PNC or LEDS promptly and that it adheres to performance standards held by the NPCC, such as timeliness in respect of entering details generated by law enforcement events
- ensuring that the organisation publishes a privacy notice explaining what personal data may be retained and how it may be used
- ensuring that information on individual rights, in respect of information gathered and retained, is made accessible to members of the public – for example, at the point of detention into custody

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that individuals who enter data into PNC or LEDS have been vetted and trained, are provided with up-to-date guidance, and remain competent in discharging that role
- monitoring and dip-sampling the work of those who enter and maintain data to ensure that information is accurate, relevant and up to date, and that it conforms to national minimum data quality standards
- ensuring that updating guidance is disseminated to, and understood by, relevant staff within the organisation to ensure that practice remains valid in line with current national guidelines on data quality and adheres to legislation governing the processing of data

Systems users

As a systems user, you are responsible for:

- entering personal data into the database only for a lawful purpose and ensuring that the law enforcement, other policing, national security or safeguarding purpose is specific, explicit and legitimate
- ensuring that the data that is entered onto the database is accurate, authentic, adequate, current and relevant to the lawful purpose
- entering data in the appropriate format and complying with nationally agreed recording standards and national minimum data quality standards
- ensuring that all required fields are complete, such as recording of protected characteristics (for example, race and gender) and vulnerability markers
- recording the origin of the information, assessing the reliability of the information, and distinguishing fact from opinion
- recording any necessary restrictions on the application of the information, to permit later review, reassessment and audit – this is subject to provision of other guidance on the use of covert surveillance or human intelligence sources

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to provide and update strategic and policy guidance across national and local information systems, to help data owners implement legal requirements in processing data
- providing and updating strategic and operational advice on the balance between collecting data that is adequate and relevant for law enforcement, other policing or safeguarding purposes, while also being able to withstand the tests of reasonableness, proportionality and necessity
- working with the Home Office to establish performance measures that align with core data-quality standards for policing

Home Office

The Home Office will support chief officers by:

- developing protocols for improving the quality of data on PNC and LEDS and on behalf of the relevant joint controllers proactively leading organisations to put in place measures to ensure that data entered onto both systems is accurate and correctly entered

- working with relevant organisations to ensure that data quality standards are refreshed to reflect changes in regulation and legislation
- working with the NPCC to publish performance standards for timeliness of data entry for both systems
- monitoring data quality in both PNC and LEDS on behalf of the Joint Controllers and providing feedback to inputting organisations based on compliance with national minimum data quality standards
- collecting and reporting on data quality, on behalf of the Joint Controllers, in line with best practice guidance

3. Amending and updating the data record

Principle

Data stored on PNC and 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 the 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 practicable.

Requirement

Data stored on PNC and 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 practicable.

Why is this relevant?

Information comes to both systems from various sources and is received in different ways. Within both PNC and LEDS, the originating or responsible organisation may share the right to update that information.

If data held on the databases is modified to make it inaccurate or incorrect, this could interfere with the fair and lawful process of justice. Data that has been entered onto either system (or originating databases) should be accurate at the point of entry, but new information may arise – for example, a missing person may be found, or an event may need to be added to a person record. This includes arrest, entry into custody and committal (or outcome of) court proceedings.

In accordance with the current **Victims' Code**, victims are entitled to receive updates within set timescales of between one and five days at key stages in their cases, including when a suspect is arrested, bailed or charged.

Errors in data, such as an incorrect or incomplete address, may be revealed during operational access. It is essential that the user can report that inaccuracy at that point, so that action can be taken to amend. In ensuring accuracy, it is important not to delete historical information that may be significant, such as details of previous addresses. This requires a whole organisational approach, processes in place to report errors, processes to act on reported errors and quality assurance of these processes.

It is essential that data conforms to national minimum quality standards. Safeguarding risks could potentially arise from the collection of poor-quality data. Inaccurate or omitted data in such cases risks serious consequences, such as allowing a convicted offender who has committed offences in relation to children to work as a carer or school employee.

Further suggested guidance

- **APP on information management**
- **APP on data protection**
- **The Code of Practice for Victims of Crime 2021**

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- ensuring that there is a systematic process for amending data to maintain the accuracy and currency of information
- ensuring that only specialist users can amend and update data and that they are appropriately trained
- ensuring that all data on discontinuance or conclusion of law enforcement proceedings is entered onto either PNC or LEDS promptly and that it adheres to performance measures held by the NPCC, such as timeliness or other core data quality standards
- ensuring that there are procedures in place to rectify errors that are reported by internal users of the systems, partner agencies or individuals who have sought access to view their data and

exercise their rights, including the right to rectification

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that people who amend data held within PNC or LEDS have been trained, are provided with up-to-date guidance, and remain competent in discharging that role
- monitoring and dip-sampling the work of those who enter and maintain data to ensure that information that migrates onto the systems is accurate, authentic, adequate, up to date, relevant to the specific, explicit lawful purpose, and entered in the appropriate format
- ensuring that errors or inaccuracies reported by frontline users are reported back to the source that created the entry for rectification
- ensuring that reported errors or inaccuracies are amended in local systems when reported back by users from national systems

Systems users

As a systems user, you are responsible for:

- ensuring that any direct changes you make to data held within the national database are accurate, relevant to the explicit lawful purpose, and entered in the appropriate format
- linking information on an individual who is the subject of an existing record appropriately to the original record and avoiding duplication of entries
- correcting inaccurate information at the point the inaccuracy is revealed or reporting the error to the data source where this cannot be directly amended
- updating information promptly into the relevant record in accordance with agreed timescales
- identifying for the local audit trail who has augmented or altered the record, when it was changed, for what purpose and on whose instigation if on request

NPCC

The NPCC will support chief officers by:

- working with the Home Office to establish performance measures for accuracy and currency of data updates by policing
- providing and updating strategic and policy guidance across national and local information systems, to help data processers understand the appropriate protocols for making amendments to

the national database

Home Office

The Home Office will support chief officers by:

- working with the NPCC, together on behalf of the joint controllers, to publish performance standards for timeliness of data amendment and updating

4. Validating the data record

Principle

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

Requirement

Data validation ensures that data is subject to a data-cleansing process, to ensure that it conforms to minimum data quality standards. The currently available data must be correct and relevant. There are key principles in both the DPA 2018 and the UK GDPR, which apply to how data is entered.

Data processing should be lawful, fair, adequate, relevant and not excessive. The data should not be kept for longer than is necessary. Data must not be processed in a manner that is incompatible with the purpose for which it was originally collected.

In line with the UK GDPR and the fourth principle of the DPA 2018, it must be accurate, complete, reliable and up to date before it is shared among agencies who require it to discharge their responsibilities.

Law enforcement data must be processed in line with the six data protection principles set out under **Part 3, Chapter 2 of the DPA 2018**. Data processed for safeguarding or other policing purposes is subject to the UK GDPR.

Why is this relevant?

Regardless of the originating agency or originating database – or how it enters the national database – validating police or law enforcement information ensures that all police or law enforcement information is processed in accordance with the law. The validation of migrated data for compliance with national minimum data quality standards is part of the data migration process in transferring data from one computer storage system to another.

This may happen in different ways for PNC and LEDS and will be an ongoing process, where police services and other agencies input data through interfaces with existing databases. Data validation can be an automated process.

The Information Assets Dashboard is a quality improvement tool created for LEDS development, which enables accurate data migration and supports organisations to improve data quality.

Further suggested guidance

- **The Information Commissioner's Office Guide to Law Enforcement Processing**

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- ensuring that provisions such as the UK GDPR and the DPA 2018 are adhered to when migrating data into the database
- ensuring migrated data is subject to appropriate validation
- confirming that personal data is processed in line with data protection legislation
- ensuring that there is a systematic process for conducting regular quality checks to confirm that data is entered accurately and correctly, conforming to national minimum data quality standards
- ensuring that there are procedures in place to rectify errors that are discovered during validation procedures
- ensuring that monitoring and dip-sampling of the work of those who enter and maintain data is carried out, in line with practice guidance on data quality, and that the results are collated and reported
- ensuring that updated guidance on data quality is disseminated to relevant managers and staff within the organisation, to ensure that practice remains valid in line with current national guidelines

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that individuals who validate data that will be entered into PNC or LEDS have been vetted and trained, are provided with up-to-date guidance, and remain competent in discharging that role
- monitoring and dip-sampling the work of those who enter and maintain data to ensure that information that migrates onto PNC or LEDS is accurate, authentic, adequate, up to date, relevant to the law enforcement, other policing or safeguarding purpose, and entered in the appropriate format

Systems users

As a systems user, you are responsible for ensuring that the data you provide is:

- accurate
- authentic
- adequate
- up to date
- relevant to the law enforcement, other policing or safeguarding purpose
- entered in the appropriate format

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to provide and update strategic and policy guidance across national and local information systems, to help data controllers and processors understand data requirements before they migrate data
- working with the Home Office, together on behalf of the joint controllers, to establish performance standards for timeliness of data validation for policing

Home Office

The Home Office will support chief officers by:

- proactively, on behalf of the Joint Controllers, leading organisations to put in place measures to ensure that data from existing databases, or inputted directly onto both PNC and LEDS, is entered accurately and correctly

- working with the NPCC, together on behalf of the joint Controllers, to publish performance standards for timeliness of data validation in business rules or manuals of guidance
- collecting and reporting on data quality, on behalf of the joint controllers, in line with best practice guidance

5. Review, retention and disposal of data

Principle

In accordance with the UK data protection regime, data stored and otherwise processed by law enforcement on 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 and 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.

Requirement

The primary purpose of review, retention and disposal (RRD) procedures is to ensure the validity and legality of the data held in PNC or LEDS. To comply with data protection principles, a regular process for review and deletion of the data should be in place in each organisation.

The privacy rights of the individual, as enshrined in legislation, should be balanced against the law enforcement requirement. To this end, the retention of police information should be determined by the level of risk presented by an individual. This risk must be clearly evidenced and fully auditable if challenged. A data subject may request the controller to erase personal data or to restrict its processing, however, the legal duties of the controller apply regardless of whether such a request is made.

Data must only be retained proportionately to the law enforcement purposes and must comply with the fifth data protection principle under Part 3, Chapter 2 of the DPA 2018 (that is, for no longer than is necessary for the purpose for which it is processed). Under section 39 of the DPA 2018, appropriate time limits for periodic review must be established and controllers, namely chief officers in policing, are accountable for that review.

Individuals also have the right to request the deletion or removal of their personal data if continued retention infringes the data protection principles. The use of data for safeguarding or other policing purposes must be lawfully processed under the UK GDPR and the same principles are applied. APP for information management recognises that a key principle is compliance with data protection legislation.

Data held on PNC is currently subject to specific NPCC issued guidance (issued on behalf of the Joint Controllers) concerning retention of convictions which will extend to LEDS.

Why is this relevant

One of the primary functions of PNC and LEDS is to ensure that data can be shared appropriately and meaningfully across police forces and law enforcement agencies. Reviewing and recording of police information and data is central to risk-based decision-making and public protection.

Data extracted from PNC or LEDS must be deleted within seven days of that extraction unless, following appropriate assessment of the need for continued retention, it is retained in accordance with national policy and procedures. Some elements may be retained for longer than other elements where justified and lawful to do so, such as to provide both an investigatory and audit thread.

The integrity of the data held on national systems will be heavily reliant on local system compliance with current policy and guidance on RRD in England, Wales, Scotland and Northern Ireland and other jurisdictions. This is specific to policing and may not be applicable to other organisations, which should ensure that they are legally compliant.

Organisations that hold local data that is not compliant with data protection principles create the risk that migrated data held on the systems could be held unlawfully. Organisations should consistently review information held and actively delete information that does not have a proportionate law enforcement, other policing or safeguarding purpose, or ensure that the rationale for any continued retention is clearly evidenced. Under the Inquiries Act 2005, it is an offence for a person to intentionally destroy or alter evidence that is likely that an inquiry would (if they knew of its existence) wish to be provided with.

It is the responsibility of the data controller or controllers for each processing operation to comply with legal requirements, and to ensure that local record deletion is reflected on both PNC and LEDS

where appropriate or required. This may be delegated to the reviewing officer or data steward or may partly be discharged by an automated process.

Further suggested guidance

- **Part 3, Chapter 2 of the DPA 2018**
- **APP on data protection**

For police services only

- NPCC Data Protection Manual of Guidance produced for police data protection professionals. This document is available to members of the NPCC Data Protection Group.

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- ensuring that regular reviews are conducted on locally held data, in accordance with the law, to ensure that personal data is not held longer than is necessary for the purpose for which it is processed and does not transfer or remain in PNC or LEDS unlawfully.
- confirming that personal data is retained in accordance with national policy and legal requirements laid down in data protection legislation
- ensuring that there is clear guidance available to members of the public as to how, and to what extent, they may exercise individual rights granted under the UK GDPR and Part 3, Chapter 3 of the DPA 2018 (the right to be informed, the right of access, the right to rectification, the right to erasure or restrict processing, and the right not to be subject to automated decision-making)
- deleting or correcting information that has been shown to be inaccurate
- deleting data (vehicle, property or other) that is no longer necessary for law enforcement purposes
- deleting biometric data (DNA and fingerprint) in compliance with the circumstances and timeframes set in place under the Protection of Freedoms Act 2012

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that individuals who review data entered into PNC or LEDS have been vetted and trained, are provided with up-to-date guidance, and remain competent in discharging that role.
- ensuring that the organisational strategy for reviewing records is implemented to ensure that such data is used in compliance with the law, and for lawful purposes.
- ensuring that regular reviews are carried out in line with national compliance guidance for RRD and that compliance checks are conducted to monitor adherence to that guidance.
- responding to any specific requests made on behalf of the controllers, to review personal information that is being held electronically on PNC or LEDS and liaising with ACRO Criminal Records Office, or another designated body, where appropriate.
- ensuring that systems users are complying with national minimum data quality principles and employing good practice when dealing with record management, including applying the appropriate guidance to each action.
- documenting and recording every review undertaken, irrespective of whether it results in any alterations or deletions.
- ensuring that appropriate records are kept, which include what information is stored where, and support the retention and disposal aspects of the procedure.

Systems users

As a systems user (reviewing officer), you are responsible for:

- conducting scheduled reviews of data held in PNC or LEDS, in line with national guidance
- updating the record if any inaccurate information is discovered or if new information is received – this ensures that the record is accurate and up to date
- ensuring that data quality standards are applied when undertaking initial reviews
- adhering to the appropriate RRD procedures and periods, in line with national guidance when determining whether policing records should be retained or deleted
- ensuring that any data marked for deletion under review is not relevant to any ongoing relevant independent inquiry and should be retained in compliance with the Inquiries Act 2005

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to set and maintain the policy guidelines for RRD of data by policing, to ensure that this is conducted in line with current legal requirements and meet the

measures of core data quality standards
- promoting compliance to the RRD processes
- working with the Home Office and regulatory bodies to monitor compliance on behalf of the joint controllers and provide assurance to all organisations

Home Office

The Home Office will support chief officers by:

- removing or restricting organisational access to data sets where this is not commensurate with a legal or safeguarding purpose and where instructed to do so by the joint controllers
- working with the NPCC and regulatory bodies, on behalf of the joint controllers, to monitor compliance and provide assurance to all organisations
- confirming, on behalf of the joint controllers, with non-police data owners that a review process is in place to ensure that legal responsibilities for reviewing and deleting are clearly defined

6. Accessing and applying the data held

Principle

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

Requirement

Data must be applied ethically to support justifiable law enforcement decisions. Decision makers should consider the principles of preventing discrimination, promoting good relations and fostering equal opportunities when using law enforcement information. Organisational access to data sets where this application is not commensurate with a legal or safeguarding purpose could be restricted or removed.

A key principle under data protection law is purpose limitation. Controllers must ensure that personal data that has been collected for a specific purpose in PNC or LEDS is not then further processed in a way that is incompatible with the original purpose. They will also need to demonstrate that this processing is proportionate and will not have a disproportionate impact on certain sections of the population.

There are additional rules that apply to ‘sensitive processing’ of some specified types of particularly sensitive personal data. Sensitive processing is defined by **section 35(8) of the DPA**.

Why is this relevant?

The details of individuals and incidents recorded on PNC and LEDS are an important source of information for application in law enforcement and other lawful purposes. Data on the two systems may be used for immediate response to incidents, operational planning, investigations, prosecutions and other law enforcement and safeguarding processes.

Data held on PNC and LEDS may be accessed to gauge the level of law enforcement response necessary and for an assessment of risk. Some forces have personnel responsible for examining data against other relevant records, as well as informing officers of any risks they are likely to face on attending the location of an incident, or when dealing with the subject of the report. One of the features of LEDS is that officers responding on the front line will be able to access more data directly than is currently possible with PNC. Accessing either system to view the records of individuals for curiosity or personal gain is a serious breach of data security and may result in prosecution.

Anyone who accesses PNC or LEDS must therefore be able to determine what is a lawful purpose – that is whether it is a policing, law enforcement or safeguarding purpose. These are defined in the **Purpose and scope of the Code and guidance**.

This will also apply to other agencies, such as the Probation Service, who may be dealing with high-risk individuals, or for example agencies who are concerned with the welfare of missing persons . This decision involves assessing the situation, including any specific threat or risk of harm, and determining whether this fits the test of lawful purpose.

Further suggested guidance

Police services who are accessing LEDS should adhere to this guidance. Other law enforcement agencies may use this as guidance in developing their own internal standards.

- **APP on intelligence management**

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- ensuring that information obtained from either PNC or LEDS is applied professionally and ethically to support justifiable policing, law enforcement and safeguarding decisions
- undertaking data and equality impact assessments for any new uses of data from PNC or LEDS
- ensuring that an appropriate policy document is in force to cover the processing of sensitive data at the time the processing takes place, as required by the DPA 2018
- providing information and statistics on the use, management and protection of data obtained through PNC or LEDS

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that those who access either PNC or LEDS data are vetted and approved
- ensuring that individuals who analyse data accessed from or processed on PNC or LEDS have been vetted and trained, are provided with up-to-date guidance, and remain competent in discharging that role
- monitoring the work of those who access data from either system to ensure that information that informs decision-making is reliable and accurate, and that it is used lawfully, professionally and ethically

Systems users

As a systems user, you are responsible for:

- using approved access to PNC and LEDS only for purposes that are lawful, proportionate and relevant
- understanding and updating knowledge of the capability, application and interrelation of data sets within the platforms, to make best use of the available data by correct application appropriate to the lawful purpose
- evaluating the information for provenance, accuracy and reliability and proportionality to the purpose of application – for example, an immediate incident requires a faster response than accessing information during an investigation
- applying recognised decision-making tools and risk analysis processes to demonstrate how information has been interpreted, conclusions drawn, recommendations made, and assessments made of possible future behaviour

- recording how the information has been applied for lawful purposes, using common terminology and in accordance with operating principles that promote common understanding around the certainty or otherwise of any judgements made
- acknowledging when information is obtained from PNC or LEDS and, where applicable, the originating dataset
- assessing and recording judgements on the reliability of the information and recording any necessary restrictions on the application of the information to permit later review, reassessment and audit
- disposing of data extracted from either PNC or LEDS in accordance with defined policy and procedures

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to provide and update strategic and policy guidance across national and local information systems, to help system users understand the appropriate protocols for applying data obtained through the platform
- working with the College of Policing to provide and update guidance to help system users report on their access and application of data
- monitoring and reporting how data from PNC and LEDS have been accessed and applied by policing in support of policing, law enforcement and safeguarding purposes
- working with the College of Policing to set and maintain the policy guidelines for application of data by policing, to ensure that this is conducted in line with current legal requirements
- working together with the Home Office (on behalf of the joint controllers), and regulatory bodies to monitor compliance and provide assurance to all organisations

Home Office

The Home Office will support chief officers by:

- working with organisations to ensure that any additional functionality and system developments meet the needs of organisations and users
- gathering information and statistics from user organisations to publish an annual report on the use, management and protection of data, accessed through PNC or LEDS
- monitoring the use of data from PNC or LEDS to ensure that it is applied lawfully, ethically, proportionately and in accordance with the purpose for which it was collected, or lawfully for

another authorised purpose
- working with the NPCC and regulatory bodies to monitor compliance and provide assurance to all organisations

7. Reporting and analysing the data held

Principle

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.

Requirement

Information obtained using data from PNC or LEDS must be identified clearly as being sourced from PNC or LEDS and reporting should follow existing protocols. Analysts must deliver effective and accurate analysis that can be understood and acted upon. Factual errors will undermine analytical products. Special considerations apply to solely automated decision-making processes, which are subject to specific provisions within the UK GDPR and the DPA 2018.

Why is this relevant?

Data held on PNC or LEDS can be analysed to:

- identify patterns in information
- identify effective practice and lessons learned through a review of tactical and strategic activity
- provide statistical data

Intelligence-led policing allows police to be proactive rather than reactive. It is used to understand crime and disorder issues, and to provide insight, clarity and context to support strategic decision-making in law enforcement and the tactical deployment of resources. In policing, intelligence analysts investigate who is committing crimes, how, when, where and why. This is done at all levels, including local, county, regional and beyond. The more joined-up data sets within LEDS will enable forces and other organisations to work effectively beyond county lines and across agencies with differing responsibilities.

Inaccurate data reporting can lead to misinformed strategic decision-making based on erroneous evidence or inefficiencies in applying resources. Incorrect analysis could therefore lead to

operational errors. Increasing potential for the use of automation in data analytics will enable policing to be more efficient in how data is organised. Caution should be exercised through applying human intervention to inhibit an adverse legal or similarly significant effect for an individual.

Further suggested guidance

- **APP on intelligence management**
- **The ICO Guide to Law Enforcement Processing – advice on right not to be subject to automated decision making**

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- ensuring that data analytics are carried out lawfully, necessarily and proportionately
- ensuring appropriate analytical approaches are used for the particular piece of analytical activity
- confirming that people who have a data analytic role are fully vetted and trained and competent in discharging that role
- ensuring staff are trained in data ethics
- providing clear guidance for their staff in the use of decision support tools, including algorithmic decision support tools

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that people who analyse data held within PNC or LEDS have been trained, are provided with up-to-date guidance, and remain competent in discharging that role
- monitoring the work of those who analyse and report on data, to ensure that information that informs decision-making is reliable and accurate

Systems users

As a LEDS user, you are responsible for:

- ensuring that data that is reported is accurate, current and statistically sound

- acknowledging when data is obtained through PNC or LEDS and, where applicable, the originating data set
- applying sound analytical techniques and decision-support systems that provide evidence to demonstrate how information has been interpreted, conclusions have been drawn, and recommendations have been made
- applying the National Intelligence Model approach as a police user to ensure common terminology and operating principles, to promote common understanding around the certainty or otherwise of any judgements
- ensuring that when applying data to conduct analysis, personal information is made anonymous where there is no justification for identifying specific individuals

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to provide and update strategic and policy guidance across national and local information systems, to help data analysts understand the appropriate protocols for applying data obtained through the national database
- working with the College of Policing to ensure that there is clear guidance in the lawful and ethical use of decision support tools in policing, including algorithmic decision support tools

Home Office

The Home Office will support chief officers by:

- ensuring that functionality and system developments enable data analytics

8. Sharing data that is held

Principle

Shared access to relevant data is essential for 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.

Requirement

Data is already shared from PNC, but LEDS has been developed so that data can be more readily shared among agencies that require it to discharge their law enforcement and safeguarding responsibilities.

There are key principles that apply to how data on PNC or LEDS may be shared effectively and lawfully, both among law enforcement agencies within the United Kingdom and across borders (across the European Union or more widely).

These are usually captured in data sharing agreements which must adhere to the UK GDPR and the DPA 2018 principles and provisions. For policing, the drafting of such agreements is subject to the Joint Controller's decision to adopt a national governance structure, whereby forces should use a national template and follow a local and national consultation process.

Sharing personal data must be carried out in accordance with UK data protection law. Part 3 of the DPA 2018 sets out the separate data protection rules for law enforcement. The UK GDPR sets out the regime for data processed for wider policing and safeguarding purposes. There is guidance set down in the ICO Guide to Law Enforcement Processing and ICO Data Sharing Code of Practice to ensure that systems and processes are in place to restrict the sharing of data, other than in compliance with legal and national policy guidelines. Certain treaties or agreements in international law may apply for sharing beyond the UK.

The data protection legislation imposes certain restrictions and safeguards in sharing for law enforcement purposes. This especially applies to sharing overseas where the destination country has not obtained an adequacy decision indicating that they provide an adequate level of protection for the rights and freedoms of data subjects. This is particularly important in the case of countries that participate in, solicit, encourage or condone the use of torture or cruel, inhuman or degrading treatment or punishment for any purpose.

Prior to departure from the European Union, UK law enforcement agencies were also party to the Schengen Information System (SIS) to share alerts on wanted or missing persons and objects. Similar measures are achievable using existing international tools, such as Interpol I-24/7 and Interpol notices. The UK government I-LEAP Programme is now working to provide a single mechanism to access and share alerts related to people, documents and objects.

Why is this relevant?

Data sharing includes disclosure by transmission, dissemination or other means of making data available. Sharing responsibly can provide accurate and joined-up information to bring offenders to justice, prevent crime and better protect the vulnerable. Organisations using either PNC or LEDS should be confident that the data available complies with the legislative and regulatory frameworks in place, has been ethically captured and is appropriate to share, in line with any data sharing agreements.

The Code assumes two main types of data sharing from the systems.

1. Routine data sharing (where specific data sets are shared between organisations for an established, proportionate and lawful purpose).
2. Decisions to share specific proportionate data upon a specific lawful request.

Joint-controller arrangements, data-processing contracts or memoranda of understanding may cover data sharing of either kind or alternatively data shares may be subject to specific data sharing agreements that assist accountable and legally compliant sharing as well as reinforce the principles set out in the Code. These will clarify whether organisations will either directly access all functionality on PNC or LEDS or will gain access to restricted data sets.

The police are permitted to supply information, documents or articles to the Home Office for use for immigration purposes (for example through section 20 of the Immigration and Asylum Act 1999). The NPCC produced guidance in 2020 specifically on the implications of data sharing for victims or witnesses where there may be immigration issues.

As a police user, applying the National Decision Model and the Code of Ethics will help police officers and staff make, examine and challenge decisions whether to share information, when requested directly. If in doubt, seek further advice. Examples of data sharing that are not legitimate include, but are not limited to, the following.

- Sharing information with colleagues when there is no permitted lawful purpose.
- Sharing information with colleagues that is not proportionate or relevant to the identified law enforcement, other policing, national security or safeguarding task.
- Sharing information externally on individuals who may be in the public eye, whether for personal gain or for other reasons, except when there is a permitted lawful purpose and a legitimate external data share.

- Sharing information externally on individuals, vehicles or other matters to assist third-party enquiries (colleagues, family members, friends or others) that are not linked to a lawful purpose.
- Sharing information externally with others, with a view to perverting the course of justice or interfering with a law enforcement purpose.
- Printing, transmitting or exporting data in a manner that could lead to unauthorised access of the information.

Further suggested guidance

- **The ICO Guide to Law Enforcement Processing**
- **ICO Data Sharing Code of Practice**
- **APP on information management**

For selected audiences

- The **Wales Accord on the Sharing of Personal Information**, as applicable to Welsh bodies. Data sharing agreements, informed by Business Rules for LEDS, will provide further guidance protocols.
- **College of Policing APP on international investigation** outlines the protocols for first responders and investigators conducting inquiries or investigation involving foreign nationals or information held overseas.

For police services only

- Force Data Protection Officers can access the NPCC Data Protection Manual of Guidance.

What do you need to do to meet this requirement?

Chief officers

As a chief officer you will be responsible for:

- creating and upholding enforceable data-sharing agreements, memoranda of understanding or data processing agreements (as appropriate) with all organisations that enable the safe and lawful onward sharing of relevant data from PNC and LEDS through third-party sharing
- ensuring that personal data obtained from LEDS is shared with another party strictly in accordance with the lawful purposes of the data-sharing organisation

- ensuring that updated guidance on data sharing is disseminated to relevant managers and staff within the organisation to ensure that practice remains valid, in line with current national and international guidelines and the law
- ensuring that data is only shared in compliance with data protection legislation, legal and policy guidance
- ensuring that there is an audit trail for onward data sharing of personal data
- following the legal obligation to report any breach of data privacy by any member of the organisation to the ICO if it is likely to result in a risk to the rights and freedoms of individuals

Operational managers

As an operational manager within the organisation, you will be responsible for:

- ensuring that processes that enable the safe and lawful sharing of data are followed by personnel with legitimate access to the platform
- ensuring that there is an audit trail in place for any sharing of data with third-party individuals or organisations, including details of the lawful basis for the transfer

Systems users

As a systems user, you are responsible for:

- ensuring that the legitimate transfer of the data, and any necessary restrictions on the use to be made of the information, are recorded to permit later review, reassessment and audit of any such data sharing
- ensuring that data obtained from the database is only shared for a lawful purpose, and that the purpose is specified and explicit – penalties for breaching this requirement could result in disciplinary action

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to provide and update strategic and policy guidance across national and local information systems, to help data owners understand legal requirements in sharing data
- creating and administering any joint-controller agreements, data-processing contracts or memoranda of understanding, on behalf of the joint-controllers

Home Office

The Home Office will support chief officers by:

- ensuring that organisations are made aware of the human rights records of countries with whom information might be shared, and ensuring that organisations have appropriate safeguards to prevent information being used to facilitate human rights abuses
- providing technical guidance on data access and sharing, and on local systems requirements

9. Accountability for and auditing of data

Principle

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.

Requirement

The DPA 2018 and the UK GDPR emphasise the principle of accountability when processing any information that falls within the definition of personal data, and that includes monitoring compliance with data protection requirements. An audit is a systematic, independent examination of organisational processes, systems and data to determine whether activities involving the processing, use and sharing of the data are being carried out in accordance with UK GDPR and DPA 2018. Other expected legal and performance standards include:

- the Code of Practice for PNC and LEDS
- the codes of connection for systems
- other information compliance standards

Organisations must have appropriate technical and organisational procedures, which include keeping sufficient logs of access to the system and records of their processing activities.

Why is this relevant

Police forces should have robust internal audit procedures and understand the risks posed by poor data quality and breaches of data security.

Audit for PNC has traditionally taken the form of compliance audit, managed through data protection compliance structures. National Compliance Audit guidance has been updated by the College of Policing.

There is a National Auditor planning audit standards for LEDS, and it is likely this guidance will extend to PNC while transition is in process. Professional standards departments whose remit might be wider than data and security protection often find themselves often acting on careless or deliberate breaches of access to data. Having an auditable record allows organisations to evidence the lawful purpose for data processing and data sharing.

The ICO also has audit powers for carrying out both consensual and compulsory audits.

Quality audit looks for incorrect data entry, duplication, consistency and other elements of the industry accepted data quality standards. The LEDS programme has initiated a Data Quality Service that is carrying out an audit of live PNC data to identify data errors prior to migration into LEDS.

Further suggested guidance

- **College of Policing briefing note for Compliance Audit**
- **A guide to ICO audits**
- **APP on data protection**

Other guidance

- ISO 90011:2018 Guidelines for Auditing Management Systems.
- The National Auditor will also provide organisations with some guidance on expected audit practice for LEDS.

What do you need to do to meet this requirement?

Chief officers

As a chief officer, you will be responsible for:

- appointing a senior manager, or Senior Responsible Officer (SIRO) who is responsible for accountability, including the strategic compliance audit programme and compliance with legislative requirements

- ensuring that a risk assessment is conducted to identify the level of risk posed to the force in relation to poor quality personal data and compliance with data security
- confirming that people who access the platform have an identified business need to carry out their current role and are appropriately vetted
- ensuring that unlawful access or use of information held on the platform can be identified
- ensuring that procedures are in place to report and hold to account unlawful access or use of information by individuals who act outside of the Code
- ensuring that there is a systematic process for conducting regular audit checks on the integrity and quality of the data held
- reviewing audit logs that confirm that access to either PNC or LEDS is limited to those with authority to access the platform, and to ensure that such access is both lawful and reasonable
- ensuring that action is taken in response to the receipt of Daily Activity Files generated by the systems to address highlighted issues of quality and adequacy
- ensuring that monitoring and dip-sampling of the work of those who enter and maintain data is carried out in line with practice guidance, and that the results are collated and reported
- compiling organisational audit reports, including findings, recommendations and action plans detailing how findings and recommendations have been addressed, to ensure that any risk has been mitigated
- providing evidence of regular auditing in accordance with nationally agreed audit standards, together with their outcomes, for external audit and inspection purpose – for example, an inspection by HMICFRS
- ensuring that updated guidance is disseminated to relevant managers and staff within the organisation, to make sure that practice remains valid in line with current national guidelines

Operational managers

As an operational manager within the organisation, you will be responsible for:

- confirming that people who have an identified business need to access the platform to carry out their current role have been appropriately vetted and trained, are provided with up-to-date guidance, and remain competent in discharging that role
- confirming that users are adhering to national and organisational guidance concerning appropriate access and use of data, and that records are maintained of their access
- monitoring and dip-sampling the work of those who enter and maintain data to ensure that information is accurate, relevant and up to date

- ensuring that updated guidance is disseminated to – and understood by – relevant staff within the organisation, to ensure that practice remains valid in line with current national guidelines

Systems users

As a systems user, you are responsible for:

- complying with all platform access requirements for either PNC or LEDS platforms set locally within an organisation and nationally
- ensuring that access to the systems is justified through approved, secure, personal access protocols and is only carried out for a lawful purpose
- entering accurate information on justification for a data check upon access to the system
- retaining evidence or information supporting the validity of system access, processing activity and associated actions, for agreed timeframes

NPCC

The NPCC will support chief officers by:

- working with the College of Policing to provide and update strategic and policy guidance across national and local information systems, to help data owners mitigate and manage risk in a timely manner
- leading policing organisations to put in place measures to protect PNC and LEDS as a national asset and mitigate the risk of corruption
- conducting audit checks at a national level to proactively maintain data security and integrity, drive compliance and support the investigation of malpractice

Home Office

The Home Office will support chief officers by:

- building the technical capability into the LEDS platform for logging access and all relevant processing activity, to allow those with the responsibility for conducting audits to make such checks, as required under data protection legislation
- working with the NPCC to determine criteria for automated reviews of data held on the systems and feeding back Daily Activity Files that address issues of data integrity
- collecting and reporting data on compliance with best practice guidance, breaches of LEDS and PNC integrity and the outcomes of disciplinary procedures

10. Training and continuing professional development

Principle

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.

Requirement

Training for PNC has been well established and forces are aware of the current arrangements. As LEDS is a new system, a package of learning will be mandatory for continuing professional development (CPD) of all users at all levels. This will be aligned to the arrangements for PNC training and the implementation of new LEDS products.

All system users require updates on system and technical changes, as well as updates on policy and governance. These evolve and change as the landscape of law, law enforcement practice, human rights, and data protection legislation and guidance also evolves and changes.

Learning will reference the Code of Practice and the more detailed responsibilities outlined within this guidance to support the lawful, ethical and professional use of both PNC and LEDS. Periodic refresher training on data protection and other associated legislation, regulations and policy guidance is also recommended.

Why is this relevant?

PNC and LEDS exist as repositories of information that can be created, amended or deleted, and as an interface to other law enforcement data sources.

LEDS will have a new interface and will require a comprehensive and accessible learning programme upon implementation. While some of the functions that apply to LEDS are carried over from precursor or feeder data systems, some will be new and may be unfamiliar to those accessing and using the system.

Police forces will be the main users of LEDS, but other law enforcement and partner organisations will also have access. In addition, some private sector organisations will also provide data for use by law enforcement and will access data for commercial operations where there is a legitimate need, for example, to prevent or detect fraud.

PNC and LEDS are powerful tools that can greatly assist law enforcement and safeguarding activity, if used properly by people with the right knowledge and skills. Complying with national expectations and a national learning strategy will ensure consistency across organisations and across roles during the transition to LEDS.

Learning for new users and CPD for existing practitioners will ensure that individuals at all levels will understand how to use both systems effectively and apply data competently and ethically, in line with the expectations of the Code.

Further suggested guidance

- The College of Policing is working with the Home Office to create the national learning strategy for LEDS, to identify the most effective ways to deliver training as a new service and to provide guidance on CPD.

What do you need to do to meet this requirement?

Chief officers

As a chief officer, you will be responsible for:

- providing or facilitating attendance at training, in accordance with agreed national standards, so that staff who carry out data functions on PNC or LEDS are fully trained and competent in discharging their role
- ensuring that there are performance review processes and CPD opportunities for staff who carry out data functions using PNC or LEDS
- providing staff with updated strategic and policy guidance concerning data functions and expected operational best practice
- ensuring that staff have sufficient time and opportunity for CPD in accessing and using the systems

Operational managers

As an operational manager within the organisation, you will be responsible for:

- confirming that people who have an identified business need to carry out data functions on PNC or LEDS are fully trained and competent in discharging their role
- ensuring that staff who access and use data through PNC or LEDS are fully trained in accordance with the national learning strategy and agreed national standards and are competent in using all relevant functionality
- ensuring that staff have sufficient time and opportunity for CPD in accessing and using data obtained through PNC or LEDS
- ensuring that system, legislation and technical updates are provided to all relevant staff in a timely fashion

Systems users

As a systems user, you are responsible for:

- keeping personal skills levels up to date by adopting an active CPD approach – accessing refresher training, proactively checking for system and legislation updates, and reading technical guidance

NPCC

The NPCC is responsible for:

- working with the College of Policing to provide and update strategic and policy guidance to help organisational data owners understand the appropriate legal, ethical, technical and practice requirements in accessing and using PNC or LEDS
- working with the College of Policing to ensure that training and learning continues to support the effective application of data by policing

Home Office

The Home Office is responsible for:

- commissioning and securing training and learning interventions to support the implementation and continuing application of PNC and LEDS as national data assets

Tags

Information management