College of Policing

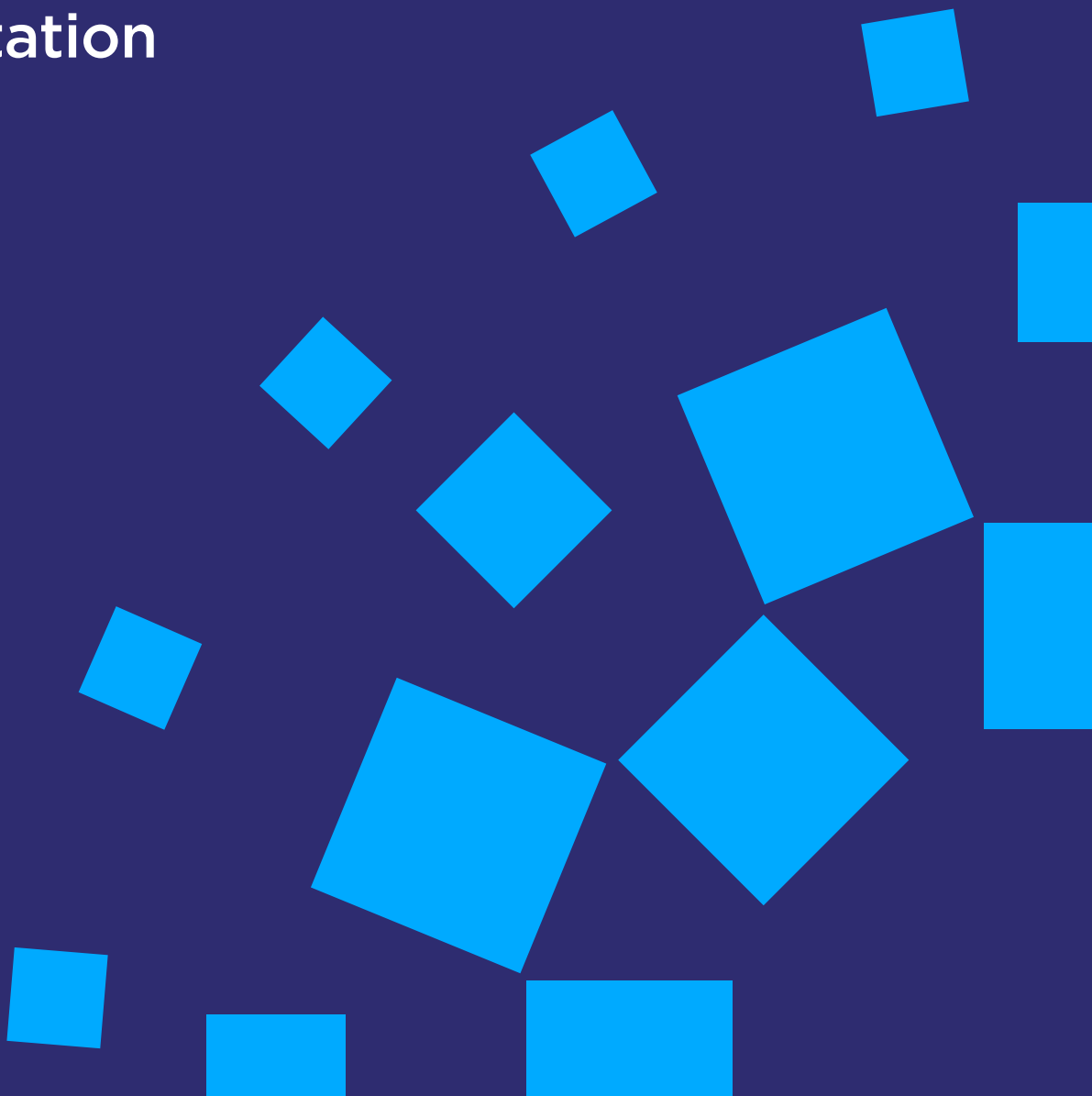
Working together to prevent crime

Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS)

Guidance part B

Consultation

2022



This publication is available for download at **college.police.uk**

If you have any enquiries regarding this publication, please contact us at **communications@college.police.uk**

This document has been created with the intention of making the content accessible to the widest range of people, regardless of disability or impairment. To enquire about having this document provided in an alternative format, please contact us at **contactus@college.police.uk**

Contents

1 Introduction 2

2 Structure of part B 4

3 Requirements of the Code of Practice 7

A. Securing the data held on LEDS 8
B. Creating the data record 14
C. Amending and updating the data record 19
D. Validating the data record 23
E. Review, retention and disposal of data 26
F. Accessing and applying the data held 31
H. Sharing data that is held 39
I. Accountability for and auditing of data access and usage 44
J. Training and continuing professional development 48

1 Introduction

1.1 This is part B of the guidance for the Code of Practice for Police National Computer (PNC) and the Law Enforcement Data Service (LEDS), which should be read together with the Code of Practice for the PNC and the LEDS (2022), as well as part A of the guidance. Part B underpins the 10 principles for the professional and ethical use of PNC and LEDS, which are set out in the Code of Practice. Taken together, these documents provide clear guidance to police forces and other organisations that access the systems. They also serve as a framework and operational context for relevant authorities, such as Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), to monitor how both systems are governed, managed and used.

1.2 The guidance is in two parts. Part A covers general guidance and part B supports the 10 principles of the Code by providing details on the reasoning behind the principles, as well as what responsibilities and actions support each one. This is relevant to all organisations that are granted access to PNC and LEDS, the managers, members and staff of these organisations, and suppliers, auditors and trainers who hold responsibilities to support those principles and understand whether they have been met. There is also a glossary of terms used across the Code and guidance documents.

1.3 The Home Office, through the National Law Enforcement Data Programme (NLEDP), has created LEDS to replace PNC. The Code of Practice covers both systems and will be in effect while users transition from PNC to LEDS, until PNC is decommissioned. Meanwhile, both systems will co-exist.

1.4 In simple terms, the Code and the guidance document provide the 'what' to do, with other existing documents referenced as existing practice guidance. Further documents will be created to elaborate on the 'how'. A comprehensive training programme is in place for PNC. Further learning and advice will also be delivered to provide

support that enables forces and other users to comply with the principles and responsibilities within the Code and guidance document while using both PNC and LEDS. Although PNC and LEDS have very different structures as data systems, they share commonality as repositories of police information. The Code and the guidance document provide a strong framework on how to ensure the secure, ethical, fair, diligent and impartial use of data for legitimate law enforcement purposes, when stored or accessed through either system.

1.5 This document references further detailed guidance that remains in place for PNC, as well as any specific guidance that is being created for the LEDS products. PNC has an user manual and set of business rules, which will be maintained until PNC is decommissioned. Some user guidance will be published for each of the LEDS products at each technical launch and this will be refreshed as the iterative development of the system progresses.

1.6 Some guidance for each of the LEDS products will be published at first technical launch and will be refreshed as the iterative development of the system progresses. For LEDS, a set of specific guidance for each product will be created, together with some overarching guidance on common themes. There will also be some performance metrics documents for both PNC and LEDS. The performance metrics may include training, data quality measures, data security and supplier requirements. For example, there were specified timeliness targets in the 2005 Code for the PNC, which will be reconsidered and refreshed. These documents will be developed by the Home Office, in conjunction with the National Police Chiefs' Council (NPCC) lead for PNC and LEDS and with the NPCC Data Board. They will be based on existing metrics and targets, such as the two for PNC, as well as identifying or developing those that are required for operational efficiency. The implementation date of the performance metrics will be three months after the document is published unless the document says otherwise.

2 Structure of part B

2.1 The operation and use of PNC and LEDS by all organisations and users must comply with the principles set out in the Code, and the guidance that supports those principles. That detailed guidance is laid out under sections 3A to 3J of this part of the guidance document, which reflect data processing functions and supporting activities in managing and using a data platform. Although PNC and LEDS users are expected to read all sections of the Code initially, it is published so that each section can be accessed and read independently. The responsibilities ascribed under each section of **Chapter 3** will be relevant to that specific data function but there may be some overlaps between sections. For example, ensuring that people who access both PNC and 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 is repeated across functions. Maintaining integrity of the platform, as well as the confidentiality and quality assurance of the data within it, are common themes that run through the sections of the Code.

2.2 Data processing, as defined in the DPA 2018, is 'an operation or set of operations which is performed on information, or on sets of information'. Broadly speaking, this includes the collection, storage and arrangement of items of data to produce meaningful information. Data processing for both systems will involve various processes or functions, including creating the data record, amending the data record, validating data, reviewing, retaining and disposing of data, accessing and applying data, disclosing or sharing data, analysing data and auditing data.

2.3 Each section of **Chapter 3** includes a short overview that identifies one of the 10 principles within the Code and explains the overall requirements that support that principle and the related data function. This includes references to specific guidance or legislation that should be read. Guidance on expected performance and practice is issued to police forces from time to

time by relevant bodies, such as the NPCC, which succeeded the Association of Chief Police Officers (ACPO) on 1 April 2015 and took over ownership of any ACPO guidance that remains current. The College of Policing, as the professional body for the 43 forces in England and Wales, sets professional standards, and produces **Authorised Professional Practice** (APP) and other guidance that support expectations of good practice. While such guidance does not have a statutory mandate, it is referenced as an indication of the standards of practice and performance to be expected of LEDS users. HMICFRS will apply the same standards to all organisations accessing PNC and/or LEDS and will use the Code and this guidance document, together with that 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.

2.4 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.

2.5 **The chief officer** of the organisation that has been granted access to PNC and/or LEDS. This may be a police force or other body that has statutory functions to exercise public authority or other responsibilities that support any of the law enforcement or safeguarding purposes. This responsibility lies with the chief officer, which, for the purposes of the Code, also includes equivalent positions in the case of other organisations using the systems.

2.6 **Operational managers** within the organisations are managers who at any level will have some responsibility for managing the operation of PNC and/or LEDS within that organisation, or the performance of personnel (staff or contractors) who may be granted access to the platform. These may occupy a specific system or data role, or may hold a wider role. Not all the responsibilities outlined will be ascribed to one individual. It is assumed that there are different individuals operating at relevant levels who will assume these responsibilities, acting on behalf of the organisation.

2.7 **A system user** is an individual who has been vetted and approved to use PNC and/or 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. Use of LEDS includes performing any data functions associated with the systems, including accessing either PNC and/or LEDS, and using the information obtained directly from them. A systems user may have a role aligned to a specific data function, such as data entry, or could be using information from the systems as part of a wider law enforcement or safeguarding role, such as a frontline police officer accessing information for operational reasons.

2.8 **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 in the United Kingdom who use PNC and/or LEDS. This guidance document ascribes responsibilities to the NPCC in relation to the strategic oversight of both systems on behalf of policing, operational use by police, and the access to – and application of – data accessed from the systems. Non-police bodies are expected to follow the same policy and practice.

2.9 **The Home Office** currently hosts the programme that is developing the LEDS platform, as well as some ongoing management of the PNC structure. Responsibilities ascribed to the Home Office for LEDS may, in due course, be adopted by a new sustainment body. The Home Office does not have statutory responsibility for many of the bodies accessing the systems but, for the purposes of this guidance, it is ascribed responsibilities in relation to its role in the governance and management of the infrastructure of the systems.

2.10 Other bodies – such as the College of Policing, which provides guidance on professional practice and learning, and the Police Digital Service – may also be referenced in respect of their relationships and responsibilities in supporting PNC and LEDS.

3 Requirements of the Code of Practice

3.1 In the following pages, the responsibilities that support each of the principles of the Code of Practice are laid out in sections. These can be read separately by those with specific interests in the principles.

A. Securing the data held on LEDS

Principle

Robust arrangements must be in place to ensure secure storage, restrictions on access, and guidance on retention and disposal of information, so that the public can have confidence in the integrity 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) if there is a likely risk to the rights and freedoms of individuals, and to do so without delay. Personal data breaches have potential for heavy financial penalty. The sixth data protection principle 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. A National Senior Information Risk Owner (NSIRO) is appointed by the NPCC to act on behalf of the joint controllers for both systems, to oversee and manage risks to the systems. In turn, each organisation that connects with PNC and/or 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, and damage to the reputations of the data owners, the NPCC and the Home Office.

Further suggested guidance

- The Home Office, on behalf of the joint controllers for PNC or LEDS, provides details of the specific technical and procedural systems requirements.
- APP on **information assurance** has been developed to support police in managing systems assurance.
- National policing Community Security Policy (CSP) National Policing Information Risk Assurance Policy.
- APP on vetting supports the **Vetting Code of Practice**.
- The Code of Practice on Police Information and Records Management 2022, particularly Principle 1, 'Governance', and Principle 4, 'Compliance'.
- The ICO website contains a wealth of guidance to support

organisations' compliance with legislation, including the **Guide to Law Enforcement Processing**.

What do you need to do to meet this requirement?

The chief officer will be responsible for:

- Ensuring that the UK GDPR and the DPA 2018 are adhered to in managing connection to PNC or LEDS at the organisational level.
- Nominating a senior manager, the SIRO, who – together with the DPO – is responsible for providing expertise and advice to assist the 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 the Governance and Information Risk Return (GIRR) process.
- Maintaining security of all 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 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 or transferring to a role that no longer warrants access.
- Ensuring that there is an audit trail for each local access event, as well as clear audit capability and processes to support maintenance of data security.

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 access is restricted by role and by relevant purpose.

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 accessing PNC or LEDS via another person's login.
- Exercising caution in printing and exporting data from the database. Hard-copy data may quickly become out of date or inaccurate and will need to be stored securely, referencing the source, date and purpose for extraction. Extracted information should be made anonymous if it is not necessary to identify personal details. Extracted information should not be retained beyond the application linked to the purpose for abstraction and should be disposed of securely.
- Maintaining personal levels of integrity, to the standard that exists for policing through the Code of Ethics.
- 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. This can include changes in marital status or civil partnership, name or address, and financial status, such as a county court judgment or participation in a debt management plan. Failing to do so may result in vetting clearance being downgraded or withdrawn.

- 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.

The NPCC will support chief officers by:

- Appointing 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 clearly defined joint-controller agreements, memoranda of understanding and data-processing contracts have been put in place on behalf of the joint controllers to provide assurance 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
- 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.

The Home Office will support chief officers by:

- Ensuring that the platform has in-built restrictions to prevent unauthorised use of PNC or LEDS or unauthorised use of specific data sets within the systems.

B. 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, and must conform to 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 national minimum data quality standards (see Part A, section 5.6). All personal data created or processed within PNC or LEDS is subject to the relevant provisions of the DPA 2018 or 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 matter of opinion or 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 product for missing persons. 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 **management of police information** and APP on **data protection**.
- **ACPO PNC Compliance Strategy (2000)**.
- The Home Office HMIC Report **Police National Computer Data Quality and Timeliness (2001)**.
- The NPCC Data Protection **Manual of Guidance** has been produced for police data protection professionals.

What do you need to do to meet this requirement?

The chief officer will be responsible for:

- Confirming that law enforcement data is processed in line with the most recent data protection legislation, and that the personal data collected for law enforcement purposes is lawful, adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Ensuring that 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 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.
- 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.

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.

As a systems user, you are responsible for:

- Entering 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.
- 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.

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 standards for timeliness of data entry for policing.

The Home Office will support chief officers by:

- Developing protocols for improving the quality of data on PNC and LEDS and 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, and providing feedback to inputting organisations based on compliance with national minimum data quality standards.
- Collecting and reporting on data quality, in line with best practice guidance.

C. Amending and updating the data record

Principle

The data stored on PNC and LEDS must be accurate and up to date while it is being used by agencies who require it to discharge their law enforcement, other policing and safeguarding responsibilities. This 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

Timeliness of updating information is critical to ensure that the database is accurate and relevant. It may be necessary to link information collected for one law enforcement purpose to other information on either PNC or LEDS, or that has been collected for a different purpose, subject to lawful authority. If there are conflicts, errors or duplications between the data sources, these need to be resolved. The UK GDPR and the DPA 2018 require that every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is either erased or rectified without delay.

Why is this relevant?

Information comes to both systems from various sources and is received in different ways. 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. Within both PNC and LEDS, the originating or responsible organisation may share the right to update that information when uploading the data into the system. 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. 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 **management of police information** and APP on **data protection** provide overall guidance on managing information in a timely and accurate manner.
- The **Code of Practice for Victims of Crime 2006** (currently subject to a review).

What do you need to do to meet this requirement?

The chief officer will be responsible for:

- Ensuring that there is a systematic process for amending data to maintain the accuracy and currency of information.
- 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 standards held by the NPCC, such as timeliness in respect of discontinuance or conclusion of law enforcement proceedings following an arrest, report or summons.

- 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.

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.

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. In ensuring accuracy, it is important not to delete historical information that may be significant, such as details of previous addresses.
- 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.

The NPCC will support chief officers by:

- Working with the Home Office to establish performance standards for timeliness of data amendment for 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.

The Home Office will support chief officers by:

- Working with the NPCC to publish performance standards for timeliness of data amendment and updating through business rules or manuals of guidance.

D. Validating the data record

Principle

The data available on PNC or LEDS must be correct and relevant. This involves validating or checking the systems (or originating databases) to ensure that the 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 processed should be lawful, fair, adequate, relevant, not excessive, and not 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.

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?

The chief officer will be responsible for:

- Ensuring that provisions such as the UK GDPR and the DPA 2018 are adhered to in migrating data into the database.
- Confirming that law enforcement data is processed in line with the six law enforcement principles set out under Part 3, Chapter 2 of the DPA 2018, and that the need to collect personal data for law enforcement purposes can be tested as lawful. Data processed for safeguarding or other policing purposes is subject to the UK GDPR.
- 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.

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 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.

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, and entered in the appropriate format.
- Ensuring that the data you enter directly into the source system is accurate, authentic, adequate, up to date, and entered in the appropriate format.

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 understand data requirements before they migrate data.
- Working with the Home Office to establish performance standards for timeliness of data validation for policing.

The Home Office will support chief officers by:

- Proactively 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 to publish performance standards for timeliness of data validation in business rules or manuals of guidance.
- Collecting and reporting on data quality in line with best practice guidance.

E. Review, retention and disposal of data

Principle

Data held 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, to ensure compliance with all legal and policy requirements and to protect the integrity of the data. There should be a formal, local governance process for the management of data with clear responsibilities.

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. 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 (i.e. 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. 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 guidance concerning retention of convictions. Other

provisions will also apply to certain data sets (see table in Part A, section 5.1).

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. Elements of the data inputted into PNC and LEDS may be retained for longer than other elements to provide both an investigatory and audit thread. The integrity of the data held on the systems will be heavily reliant on local compliance with current policy and guidance on RRD.

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. It is the responsibility of the data controller for each organisation to comply with legal requirements, and to ensure that record deletion is reflected on both PNC and LEDS. This may be delegated to the reviewing officer or data steward or may partly be discharged by an automated process.

Further suggested guidance

- The Code of Practice on Police Information and Records Management 2022, particularly Principle 6, 'Review and retention' and Principle 7, 'Disposal'.
- Part 3, Chapter 2 of the **DPA 2018**. APP on data protection and the NPCC **Data Protection Manual of Guidance**.

What do you need to do to meet this requirement?

The chief officer will be responsible for:

- Ensuring that regular reviews are conducted, in accordance with guidance, to ensure that personal data does not remain in PNC or LEDS longer than is necessary for the purpose for which it is processed.
- 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. A data subject may request the controller to erase personal data or to restrict its processing. However, the duties of the controller under this section apply regardless of whether such a request is made.
- Deleting data (vehicle, property or other) that is no longer necessary for law enforcement purposes. 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.
- Deleting biometric data (DNA and fingerprint) in compliance with the circumstances and timeframes set in place under the Protection of Freedoms Act 2012.

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 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 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.

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 and any retention schedule published by the NPCC, when determining whether policing records should be retained or deleted. This guidance is specific to policing and may not be applicable to other organisations, which should ensure that they are legally compliant.
- 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. It is an offence under that Act for a person to destroy or alter evidence that may be relevant to an inquiry.

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.
- Promoting compliance to the RRD processes.
- Working with the Home Office and regulatory bodies to monitor compliance and provide assurance to all organisations.

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.
- Working with the NPCC and regulatory bodies to monitor compliance and provide assurance to all organisations.
- Confirming with non-police data owners that a review process is in place to ensure that legal responsibilities for reviewing and deleting are clearly defined.

F. Accessing and applying the data held

Principle

All data held on PNC or LEDS must be used lawfully, professionally and ethically, in accordance with 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. 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. There are additional rules that apply to 'sensitive processing' of some specified types of particularly sensitive personal data. This is defined by section 35(8) of the DPA 2018 and Article 5(1)(b) of the UK GDPR.

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 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. This may also apply to other agencies, such as the Probation Service, in dealing with high-risk individuals. This analytical stage involves assessing the

situation, including any specific threat or risk of harm. 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.

Further suggested guidance

- APP on intelligence management. 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.

What do we need to do to meet this requirement?

The chief officer will be responsible for:

- Ensuring that information obtained from either PNC or LEDS is applied professionally and ethically to support justifiable law enforcement decisions. Organisational access to data sets where this application is not commensurate with a legal or safeguarding purpose could be restricted or removed.
- Undertaking data and equality impact assessments for any new uses of data from PNC or LEDS, to demonstrate that personal data that has been collected for a specific purpose in LEDS is not then further processed in a way that is incompatible with the original purpose. This will also demonstrate that this processing is proportionate and will not have a disproportionate impact on certain sections of the population.
- 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.

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 entered into 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 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.

As a systems user, you are responsible for:

- Using approved access to PNC and LEDS only for purposes that are lawful, proportionate and relevant to a law enforcement, other policing, national security or safeguarding task. 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.
- 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. This permits later review, reassessment and audit.
- Disposing of data extracted from either PNC or LEDS in accordance with defined policy and procedures.

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.
- Promoting compliance to the RRD processes.
- Working with the Home Office and regulatory bodies to monitor compliance and provide assurance to all organisations.

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.

G. 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 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 a provision that exists 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, to identify effective practice and lessons learned through a review of tactical and strategic activity, and to 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. However, without human intervention, this may result in an adverse legal or similarly significant effect for an individual.

Further suggested guidance

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

What do we need to do to meet this requirement?

The chief officer will be responsible for:

- Ensuring that data analytics are carried out lawfully.
- Confirming that people who have a data analytic role are fully trained and competent in discharging that role.
- Providing clear guidance for their staff in the use of decision support tools, including algorithmic decision support tools.

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.

As a LEDS user (data analyst), 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.

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.

The Home Office will support chief officers by:

- Ensuring that functionality and system developments enable data analytics.

H. Sharing data that is held

Principle

Data from PNC or LEDS must be processed lawfully and ethically. Shared access to data is essential for discharging law enforcement, other policing, national security or safeguarding purposes.
The Code seeks to encourage the lawful and effective disclosure of data to better support law enforcement and public protection.

Requirement

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). Sharing personal data must be carried out in accordance with data protection law. Part 3 of the DPA 2018, which sets out the separate data protection rules for law enforcement, and the **UK GDPR**, which sets out the regime for data processed wider policing and safeguarding purposes, will be relevant. The data protection legislation requires restrictions and safeguards in sharing overseas for law enforcement purposes, particularly where there is no guarantee of an adequate level of protection for the rights and freedoms of data subjects. Prior to departure from Europe, UK law enforcement agencies were also party to the Schengen Information System (SIS) to share alerts on wanted or missing persons and objects, both inside the EU and at the EU external border. Similar measures are, however, achievable using existing international tools, such as **Interpol I-24/7** and **Interpol notices**.

Why is this relevant?

Data is 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.

Data sharing includes disclosure by transmission, dissemination or other means of making data available. Sharing responsibly will 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. The Code assumes two main types of data sharing from the systems: routine data sharing (where data sets are shared between organisations for an established purpose), or decisions to share data upon a specific request.

Joint-controller arrangements, data-processing contracts or memoranda of understanding should cover both aspects, assist accountable sharing and reinforce the principles set out in the Code. The police are permitted (section 20 of the Immigration and Asylum Act 1999) to supply information, documents or articles to the Home Office for use for immigration purposes. The NPCC produced guidance in 2020 specifically on the implications of data sharing for victims or witnesses where there may be immigration issues.

Further suggested guidance

- The ICO **Guide to Law Enforcement Processing** and the ICO Data Sharing Code of Practice.
- APP on **information management**, which covers sharing police information linked to a policing purpose.
- The national Information Management Coordination Committee and the **NPCC Data Protection Manual of Guidance** provide guidance to forces in England and Wales.
- 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.

What do you need to do to meet this requirement?

The chief officer will be responsible for:

- Creating and upholding enforceable data-sharing agreements with all organisations that enable the safe and lawful onward sharing of data from LEDS through third-party sharing. These must adhere to the UK GDPR and the DPA 2018 principles and provisions. For policing, the drafting of such agreements is subject to a national governance structure, whereby forces should use a national template and follow a local and national consultation process.
- Ensuring that personal data obtained from LEDS is only disclosed to another party that does not itself have access to LEDS, to support the lawful purposes of the organisation accessing LEDS.
- 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.
- Ensuring that data is only shared in compliance with data protection legislation, legal and policy guidance. For example, complying with the guidance set down by the ICO Guide to Law Enforcement Processing and ICO Data Sharing Code of Practice in ensuring that systems and processes are in place to restrict the sharing of data, other than in compliance with legal and national policy guidelines.
- Identifying Schengen-sourced data and applying controls set out in the SIS II Regulations, while these are in place.
- Reporting 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.

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.

As a LEDS 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. 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 for a purpose that is not a specific law enforcement, other policing, national security or safeguarding task.
    - 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.
    - 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.

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 that is:
  - relevant for law enforcement, other policing or safeguarding purposes
  - appropriate for sharing among other law enforcement agencies
  - appropriate to other specific organisations
  - of interest to European and other overseas jurisdictions

The Home Office will support chief officers by:

- Ensuring that joint-controller arrangements, data-processing contracts or memoranda of understanding clarify whether organisations will either directly access all functionality on LEDS or will gain access to restricted data sets.
- 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, especially with countries that participate in, solicit, encourage or condone the use of torture or cruel, inhuman or degrading treatment or punishment for any purpose.
- Providing technical guidance on data access and sharing, and on local systems requirements.

I. Accountability for and auditing of data access and usage

Principle

Data protection legislation places the accountability on controllers to demonstrate that their data protection measures are sufficient. There must be a robust audit regime in place for both PNC and LEDS to support accountability. This includes logging access and recording processing activity.

Requirement

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 the UK GDPR, DPA 2018 and other expected performance standards, such as the Code of Practice for the PNC and the LEDS, the Code of Connections for both systems or 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 have internal audit procedures and national audit guidance is evolving for the use of PNC. There is a National Auditor planning audit standards for LEDS. Forces often work through professional standards departments whose remit might be wider than data and security protection but 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.

Further suggested guidance

- The PNC Code of Connection.
- APP on **data protection**. Police services accessing PNC or LEDS should adhere to this guidance. Other law enforcement agencies can access the APP document and use this as guidance in developing their own internal standards.
- The National Auditor will also provide organisations with some guidance on expected audit practice for LEDS.
- The ICO has published **A guide to ICO audits**.
- ISO 90011:2018 Guidelines for Auditing Management Systems.

What do you need to do to meet this requirement?

The chief officer will be responsible for:

- Appointing a senior manager who is responsible for accountability, including the strategic audit programme, for compliance with audit across the organisation.
- 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 and 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 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 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS).
- Ensuring that updated guidance is disseminated to relevant managers and staff within the organisation, to ensure that practice remains valid in line with current national guidelines.

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.

As a LEDS 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.

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.

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.
- Collecting and reporting data on:
    - compliance with best practice guidance
    - breaches of LEDS and PNC integrity
    - the outcomes of disciplinary procedures

J. 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, which evolve 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 (by volume) of LEDS, but other law enforcement and partner organisations will also have access. In addition, some private sector organisations will also have access, to provide data used by law enforcement and in their 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?

The chief officer 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.
- 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.

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.

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.

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.

About the College

We're the professional body for the police service in England and Wales.

Working together with everyone in policing, we share the skills and knowledge officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help those in policing develop the expertise needed to meet the demands of today and prepare for the challenges of the future.

college.police.uk

Follow us
@CollegeofPolice

C000I0322