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

Sets out the basic principles in relation to the ethical and professional processing of data and information managed through either or both PNC and LEDS.

18 mins read

First published 23 February 2023

1. Introduction

This Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) is issued by the College of Policing, with the approval of the Secretary of State, under section 39A of the Police Act 1996. This Code applies to every chief officer (**see Note 1**) of a police force in England and Wales who has access to the PNC and LEDS in connection with the discharge of their functions. Every chief officer must have regard to this Code of Practice ('the Code') in discharging any function to which the Code relates (**see Note 2**). The Code is also available for adoption by other law enforcement agencies, including police forces in Northern Ireland and Scotland, and other UK police forces not covered by the definition set out in **section 4** below.

The PNC provides police and law enforcement agencies with access to a centralised source of information concerning individuals, property and vehicles, gathered and used for law enforcement, policing and safeguarding purposes (**see section 5** below for definitions of these purposes). The Home Office, through the National Law Enforcement Data Programme (NLEDP), is developing LEDS to replace PNC. The NLEDP is relocating the multiple existing data sets (products) currently captured within PNC into a new technology platform in LEDS. The development work on LEDS will, in due course, result in the decommissioning of PNC. Meanwhile, both systems will co-exist, and some data may appear on both. LEDS is developing through an incremental approach, which will allow the further addition of data sets.

For the purposes of the Code, the terms 'data' and information are both used in the following context. Data is a term often used for facts or figures that provide the source of information. Once the data is processed (organised, structured or presented), it can be considered a component of

information, as in ‘police information’. Therefore the Code applies to all information stored within PNC and LEDS as this is comprised of data. This will include criminal record data, personal data and special categories of personal data (as defined in data protection legislation).

This Code replaces the Code of Practice for the Police National Computer (2005) (**see Note 3**). It applies to the management of data and information through either or both systems (PNC and/or LEDS) until the closure of PNC. The Code provides a framework and operational context for relevant authorities, such as His Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), to monitor how information within PNC and LEDS is created, accessed, applied, shared, reviewed and deleted. It is supplemented by the Guidance Document for the Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS) (‘the guidance document’), which provides detail on how managers and users can support their chief officers in complying with the requirements of the Code.

The College of Policing has consulted with stakeholders, such as the National Crime Agency (**see Note 4**) and the National Police Chiefs’ Council (NPCC), as well as with the public, before issuing this Code.

2. Statutory basis of the Code

This Code has been issued by the College of Policing with the approval of the Secretary of State for the Home Department. It is made under section 39A of the Police Act 1996, which allows the College of Policing, with the approval of the Secretary of State, to issue codes of practice relating to the discharge of their functions by chief officers of police, if the College of Policing considers that:

- it is necessary to do so to promote the efficiency and effectiveness of police forces generally
- it is necessary to do so to facilitate the carrying out of joint or coordinated operations by members of any two or more police forces
- it is for any other reason in the national interest to do so

This Code, in addition to replacing the Code of Practice for the Police National Computer (2005), extends the scope of the Code beyond the PNC to also cover LEDS under the power provided by section 39A(1).

3. The purpose of the Code

Having regard to the powers conferred by section 39A of the Police Act 1996 (**see section 2**) the College of Policing believes that this Code is necessary to:

- promote the efficiency and effectiveness of police forces by supporting the ethical, fair and diligent use of information accessed from PNC and LEDS
- ensure that chief officers adopt consistent and effective practices in working individually and together as joint controllers to manage information within PNC and LEDS
- support national and public interests by endorsing the ethical, fair and diligent use of information accessed from PNC and LEDS

The aim of this Code is to provide public confidence in the legitimacy and integrity of information that is available through PNC or LEDS and the lawful purposes for which this is applied. The Code will do this as follows:

- Safeguarding people: Facilitating the appropriate use of accurate data by police and law enforcement agencies to bring offenders to justice, prevent crime and protect vulnerable people. This includes helping agencies to locate those who are missing and to safeguard people who may be vulnerable.
- Promoting accountability: Ensuring that each activity undertaken in relation to PNC or LEDS has a clear line of responsibility. Each organisation that processes data (including by supplying it) should demonstrate that they understand and comply with the principles that support the Code. The Code encourages transparency in how data that is gathered and applied for law enforcement, policing and safeguarding purposes is used, managed and disposed.
- Promoting understanding: Enabling greater understanding of the legitimate purposes for processing data, including personal data, by law enforcement. The Code uses plain language so that users of both systems, as well as the wider public, can be confident in understanding how data can be appropriately used to support the prevention, investigation, detection or prosecution of criminal offences, to protect the public and to safeguard vulnerable people. Members of the public should feel reassured that the Code reinforces specific safeguards for

the use of personal data by law enforcement to help to protect their data and privacy interests.

- Enabling performance: Continually improving the value of the information accessed and applied from PNC or LEDS by promoting high standards of data quality, ensuring the relevance of the information and strengthening partnership working where information is shared between organisations. This will be facilitated by training new users and by a requirement for organisations to proactively support relevant continuing professional development among all PNC and LEDS users.
- Promoting fairness: The public needs confidence in the integrity of data processing by law enforcement and needs to have faith that it is compliant with the law. The processing of personal data by law enforcement and policing must in particular be lawful, fair and consistent with data protection principles. Information created and retained by law enforcement must be proportionate, lawful, accountable, ethical and necessary. The Code supports the mechanisms (training, learning, management, audit and inspection) that will ensure information, including personal data, is not used in a discriminatory or unethical manner. The Code will be regularly reviewed so it is consistent with the law and evolving human rights, data protection and ethical standards.

To support these aims, the Code reflects current data protection and human rights legislation. The use of all data systems should be compliant with UK data protection legislation. The Code should also be read together with any relevant Information Commissioner’s Office (ICO) guidance on general and law enforcement processing.

Article 8 of the European Convention on Human Rights provides a right for respect for an individual’s private and family life, his home and his correspondence, subject to certain restrictions. All interferences with this right need to be lawful and necessary, and must be in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. This will include discharging particular responsibilities to consider the impact of data processing on the rights of children and other vulnerable groups. Children are entitled to specific protection regarding their personal data. Chief officers should ensure that all decisions made in relation to the processing of data within and from PNC or LEDS are lawful, ethical, proportionate and necessary. By doing so, the public can have confidence in the way that personal data is accessed and managed for law enforcement, policing and safeguarding purposes.

4. Scope of the Code

This Code applies directly to:

- the chief constable, in relation to a police force maintained under Section 2 of the Police Act 1996
- the Commissioner of Police of the Metropolis, in relation to the Metropolitan Police Service
- the Commissioner of Police for the City of London, in relation to the City of London police force

A chief officer of police (**see Note 5**) must have regard to the Code in discharging any function to which a code of practice issued under section 39A relates.

The Code is available for adoption by other law enforcement agencies, including police forces not covered by the definition set out in **section 4** above, including Police Scotland, Police Service of Northern Ireland and those in other local jurisdictions. These agencies access PNC and LEDS by written agreement.

Applications for access by non-police organisations are subject to a transparent approval process. This includes some commercial organisations, which may access PNC or LEDS under data-sharing agreements with limited access to redacted or filtered data to support law enforcement purposes, such as checking for vehicle theft or fraud. This process is governed by an information access panel, led by the NPCC-appointed information asset owner on behalf of the joint controllers.

While these agencies and organisations are not required by section 39A to have regard to the Code, compliance will be required as part of the access arrangements that provide these agencies and organisations with access to PNC and LEDS. All references to chief officer should therefore be read as a reference to the equivalent responsible individual of any user agency or organisation who connects through written agreement.

The Code recognises that there is an existing legal framework (including data protection legislation and human rights law) that governs the processing of data held on both PNC and LEDS, including creation, storage, sharing and other activities. It is the responsibility of all user agencies and organisations to always operate in accordance with the most recent legislation, as updated or revised. The guidance document provides further detail on how the legal framework operates.

Data protection legislation identifies certain organisational responsibilities and roles in the processing of personal data. The data controller decides the purposes and means of the processing activities. This may be a natural or legal person, a public authority, agency or other body, alone or jointly with others. Joint controllers must arrange between themselves who will take primary responsibility for complying with UK data protection obligations, and in particular the fairness and transparency obligations and individuals' rights. More information on the different data protection responsibilities of organisations and the associated roles is available through the website of the Information Commissioner and in the guidance document.

Under data protection legislation data controllers are responsible for their own data, but there are more complex relationships and different access arrangements for the shared systems of PNC and LEDS, that involve multiple controllers. The NPCC acts as a coordinating body for chief officers of police across the United Kingdom through an agreement made under section 22A of the Police Act 1996. This coordination role of the NPCC for both PNC and LEDS is therefore important for the efficient and effective use of both these systems, and for the management of access arrangements.

Chief officers must ensure that anyone under their direction and control processes data through PNC or LEDS in accordance with the 10 principles of the Code (**see section 6**) and the appropriate data protection provision.

All the organisations that access PNC and/or LEDS will commit in writing to operate in line with the principles set out in this Code, to comply with the requirements of a Code of Connection for each of the systems, and to report against associated performance metrics.

This Code should be read in conjunction with the guidance document. The guidance document provides further information about the 10 principles and explains how managers of user organisations and staff who are direct users can support their chief officers in relation to the Code.

5. Policing, law enforcement and safeguarding purposes

It is a requirement of this Code that chief officers6 will ensure that they, and those under their direction and control, will use information accessed through PNC or LEDS in compliance with the existing regulatory and legislative framework. There are key pieces of legislation that govern what data can be recorded, the standard it must be recorded against, how that data can be used and

how it should be managed.

This Code concerns the use of data that is captured within PNC or LEDS primarily for law enforcement purposes, but also wider policing and safeguarding purposes.

The definition of law enforcement purposes under section 31 of the DPA 2018 is adopted by this Code:

> *The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*

Policing purposes are defined for the purposes of this Code as:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice
- any duty or responsibility of the police arising from common or statute law

The Code also addresses the processing of data to safeguard children and vulnerable adults. This processing is referred to as being for safeguarding purposes, a term that encompasses protection of the health, wellbeing and human rights of individuals at risk, enabling them to live safely, free from abuse and neglect.

Under the primary UK legislative framework for data protection, processing of personal data for law enforcement purposes is treated differently from processing of personal data for other purposes. The guidance document provides further information on how data processing for wider policing or safeguarding activities is considered under current data protection legislation. Processing for analysis or research purposes of both PNC and LEDS data will continue to support both law enforcement and policing purposes. It is essential that all PNC and LEDS users understand the lawful bases for the processing of data and have access to data protection specialists for advice.

6. Ten principles for the ethical and professional use of data and information

The Code sets out 10 principles that should be applied in the context of PNC and LEDS. These principles are underpinned by current data protection principles and have regard to the seven principles of public life (‘Nolan Principles’) and the ethical standards for policing.

1. Securing the data held on systems

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

2. Creating the data record on PNC or LEDS

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

3. Amending and updating the data record

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

4. Validating the data record

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

5. Review, retention and disposal of data

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

6 Accessing and applying the data held

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

7. Reporting and analysing the data held

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

8. Sharing data that is held

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

9. Accountability for and auditing of data access and usage

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

10. Training and continuing professional development

Regular training and learning will ensure system integrity, better protection of data subjects' rights and better outcomes for law enforcement. Arrangements must be in place within all user

organisations to train new users and proactively support continuing professional development, to ensure that the highest levels of data literacy are achieved and maintained.

7. Compliance and malpractice

The Code may be considered in a court of law and referenced in disciplinary proceedings. The Code may be considered by those who hold users to account for data management practice in a law enforcement or safeguarding context – for example, the ICO or the Independent Office for Police Conduct (IOPC). HMICFRS will consider the Code in discharging its statutory responsibilities in respect of police forces in England and Wales, and similar arrangements will be in place for forces in Scotland and Northern Ireland, by agreement. Through written agreement, all user organisations will be required to co-operate with monitoring arrangements, which may include potential inspection by HMICFRS.

Chief officers must ensure that anyone under their direction and control that uses information from PNC or LEDS for law enforcement, policing or safeguarding purposes is aware of the potential consequences should they fail to act in accordance with the principles as set out in the Code or the relevant legislation. While chief officers may delegate the execution of their responsibilities to senior managers, such as a senior information risk owner (SIRO) or data protection officer (DPO), they will remain responsible for any failures of the organisation in respect of compliance with the Code and relevant legislation.

Chief officers, working together as joint controllers, must establish an effective governance framework that ensures that both PNC and LEDS are used lawfully, ethically and professionally. This should build upon data protection compliance structures.

In addition to their statutory obligations in relation to whistleblowing, chief officers must comply with national arrangements that have been put in place to protect those who express concerns about the misuse of information accessed through the systems. The existence of the local whistleblowing arrangements will be part of the inspection regime. It is a condition of access to both systems that HMICFRS have powers to inspect other law enforcement organisations that have access to both systems, as well as police forces. Other bodies, such as the Biometrics and Surveillance Camera Commissioner or the IOPC, will also have an interest in how this Code is applied. As LEDS develops, further consideration may be given to additional oversight arrangements.

Where appropriate, the whole or any part of the Code may be revised in accordance with section 39A(2) of the Police Act 1996. The College of Policing, working with the NPCC and supported by the Home Office, will undertake an annual review of the Code until LEDS becomes fully functioning and PNC is decommissioned. Review will continue regularly thereafter and will consider changes in the function and use of both PNC and LEDS as time advances. This will also reflect changes to legislation and guidance, as well as changes to the application of data held within the systems. All revision will include a formal consultation process.

Notes

1. This Code applies directly to chief officers as defined in section 101 of the Police Act 1996 (as amended).
2. As required by section 39A(7) of the Police Act 1996.
3. The Code of Practice for the Police National Computer (2005) was issued under the text of section 39A(1) of the Police Act 1996 as it stood prior to the amendments made by section 124(5) of the Anti-social Behaviour, Crime and Policing Act 2014. Section 39A(2) of the Police Act 1996 (as amended) allows the College of Policing, with the approval of the Secretary of State, to revise the whole or any part of a code of practice issued under section 39A.
4. As required under section 39A(4) of the Police Act 1996 (as amended).
5. Chief officers under direct application are defined in section 101 of the Police Act 1996 (as amended).

Fersiwn Cymraeg

- **Cod Ymarfer ar gyfer Cyfrifadur Cenedlaethol yr Heddlu PNC a LEDS (pdf) 182.43 KB**

Tags

Information management