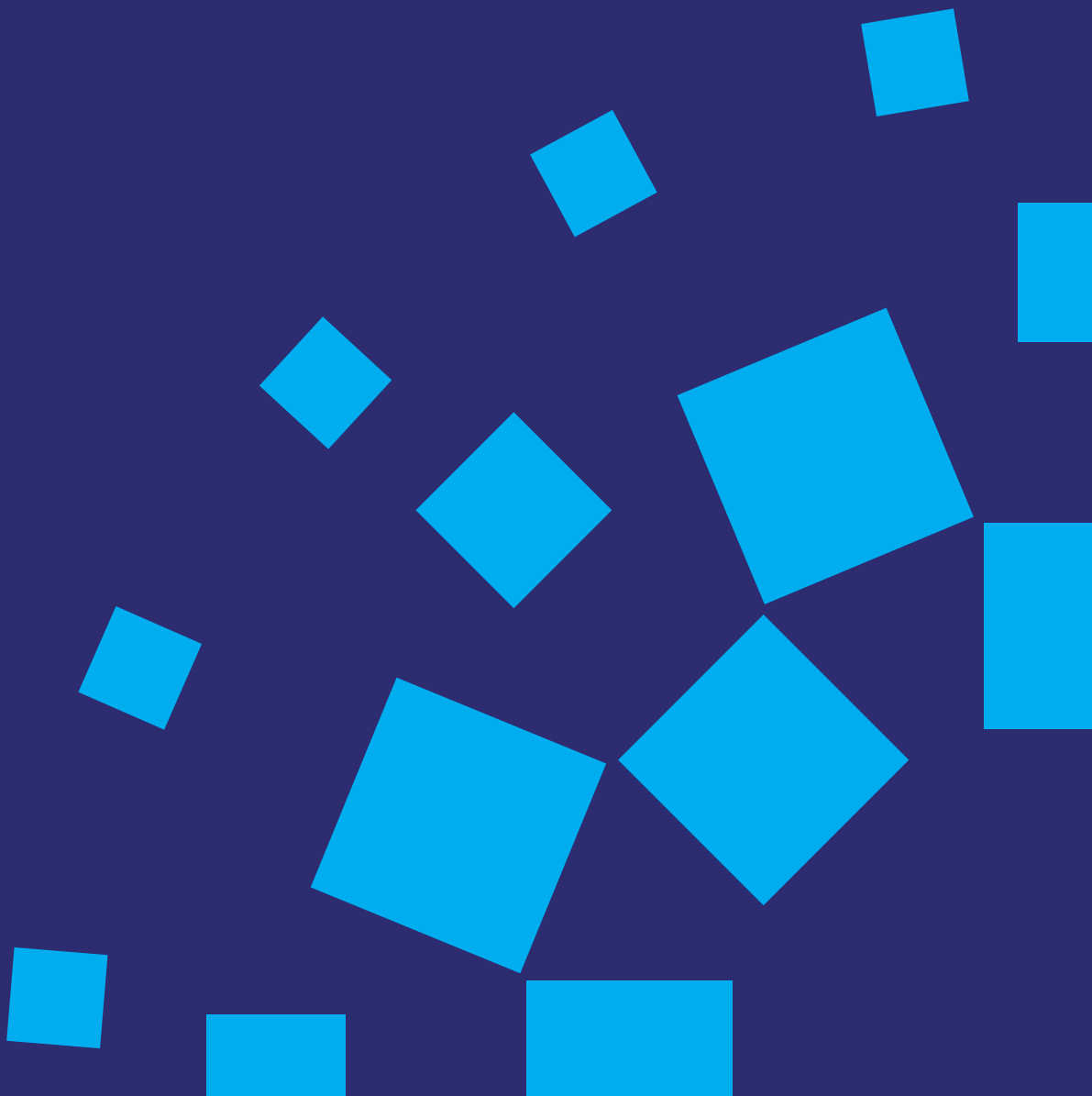
College of Policing

Working together to prevent crime

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

Consultation

2022



This page is intentionally blank

College of Policing

Working together to prevent crime

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

Contents

1 Introduction

1.1 The 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' of a police force in England and Wales who has access to 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. 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 3.2** below.

1.2 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 5.1-5.5** 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 a product-centric approach, which will allow the addition of further data sets later. For the purposes of the Code, the term 'data' is used for facts or figures that provide the source of information, including personal data. Once the data is processed (organised, structured or presented), it will be considered information for the application of the Code.

1.3 This Code replaces the Code of Practice for the Police National Computer (2005). It applies to the management of data and information through either or both systems (PNC and/or LEDS) until the closure of PNC.

1.4 The Code provides a framework and operational context for relevant authorities, such as Her 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 guidance document also clarifies some responsibilities for the Home Office as the manager of the systems.

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

2 The purpose of the Code

2.1 The purpose of the Code and guidance document is to:

- promote the lawful and fair use of the data and information managed within PNC and LEDS
- ensure that chief officers adopt consistent and effective practices in using the information obtained from PNC and LEDS
- support the ethical, fair and diligent use of information accessed from PNC and LEDS

The Code is underpinned by data protection and human rights legislation. It is consistent with the data protection principles and has regard to the seven principles of public life ('Nolan Principles') and the Code of Ethics for Policing. It should also be read together with any relevant Information Commissioner's Office (ICO) guidance on general and law enforcement processing, and with the Code of Practice on Police Information and Records Management 2022.

2.2 The aim of this Code and the guidance document is to provide public confidence in the legitimacy and integrity of information that is available through PNC or LEDS. 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, so each organisation that supplies or processes data can 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 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 better 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 continuing professional development among all 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 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 and the guidance document support 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 evolving human rights, data protection and ethical standards, such as the Code of Ethics for policing.

2.3 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. 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.

3 Statutory basis of the Code

3.1 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

3.2 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

3.2.1 A chief officer of police must have regard to the Code in discharging any function to which a code of practice issued under section 39A relates.

3.2.2 The Code is available for adoption by other law enforcement agencies, including police forces not covered by the definition set out in **section 3.2** above.

3.3 The Code recognises that there is an existing legal framework in 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 organisations to always operate in accordance with the most recent legislation, as updated or revised. The guidance document references

current legislation, such as the Data Protection Act (DPA) 2018, the UK General Data Protection Regulation and the Human Rights Act 1998. The guidance document also provides further detail and direction on how the legal framework operates.

3.4 Data protection legislation identifies certain organisational responsibilities and roles in the processing of personal data. The 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.

4 Scope of the Code

4.1 The Code is directly applicable to police forces maintained for the police areas of England and Wales, as set out in section 1 of the Police Act 1996. Other police forces not covered by section 1 of the Act (including Police Scotland, Police Service of Northern Ireland and those in other local jurisdictions) access PNC and LEDS by agreement.

4.2 All organisations access PNC or LEDS under terms of controller or joint-controller arrangements. All chief officers are controllers for their forces, but there are more complex relationships and different access arrangements for the shared systems of PNC and LEDS. 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. The NPCC has a role in providing leadership and direction to police forces in the United Kingdom who will use PNC and/or LEDS. The 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.

4.3 Law enforcement agencies or other agencies that exchange information with the police service in England and Wales will access data sets within PNC or LEDS through data processing contracts or memoranda of understanding, issued on behalf of the joint controllers. These written agreements take account of the different types and sources of data, the different purposes of the processing and the status of organisations in terms of data protection legislation.

4.4 Applications for access by non-police organisations are subject to a transparent approval process. The written access agreements specify which data sets may be made available and the purposes for which data may be applied. 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.

4.5 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.

4.6 Chief officers must ensure that anyone under their direction and control that uses information managed through PNC or LEDS for law enforcement purposes, policing or safeguarding purposes (**see 5.1**) does so in accordance with the 10 principles of the Code (**see 6.1-6.10** below).

4.7 This Code should be read in conjunction with the guidance document. The guidance document details the requirements that support the 10 principles. Chief officers are required to ensure organisational compliance with that guidance. The guidance document also clarifies how managers of user organisations and staff who are direct users will have responsibilities to support their chief officers in relation to the Code.

4.8 The guidance document also assigns responsibilities to both the Home Office and the NPCC in relation to the strategic oversight of both PNC and LEDS, their operational use by police (and other organisations), and application of information sourced through these systems.

5 Policing, law enforcement and safeguarding purposes

5.1 It is an expectation of this Code that chief officers, as well as 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.

5.2 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.'

5.3 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

5.4 The Code also addresses processing of data in safeguarding children and vulnerable adults. These are referred to as 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.

5.5 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.

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

6.1 Securing the data held on systems

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.

6.2 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, 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.

6.3 Amending and updating the data record

The data stored on PNC or 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.

6.4 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.

6.5 Review, retention and disposal of data

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.

6.6 Accessing and applying the data held

All data held on PNC and LEDS must be used lawfully, professionally and in accordance with human rights and equality legislation.

6.7 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.

6.8 Sharing data that is held

Data held within PNC or LEDS must be processed lawfully and ethically. 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.

6.9 Accountability for and auditing of data access and usage

Data protection legislation places obligations on controllers to demonstrate that their data protection measures are sufficient. This includes logging access and recording processing activity.

6.10 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

7.1 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.

7.2 Chief officers should ensure that anyone under their direction and control that uses information from PNC or LEDS for law enforcement, policing or safeguarding purposes does so following the principles set out in the Code and the relevant legislation. Chief officers should also ensure that those users are 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), they will remain responsible for any failures of the organisation in respect of compliance with the Code and relevant legislation.

7.3 The guidance document refers to specific legal requirements, such as compliance with the DPA 2018 or the deletion of DNA profiles and fingerprints under the Police and Criminal Evidence Act 1984, as amended by the Protection of Freedoms Act 2012. Any breaches of these requirements should be treated in accordance with the relevant legislation.

7.4 There must be 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. Details on how the governance framework operates can be found in the associated guidance document.

7.5 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.

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

This page is intentionally blank

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

CCS TBC
000-0-0000-0000-0 TBC

C6310322