# Purpose and scope of the Code and guidance

Purpose of the Code of Practice and the guidance for PNC and LEDS.

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

# Purpose of the Code and guidance

## Code of Practice

The purpose of the Code, as derived from powers under S39A of the Police Act 1996 and supported by this guidance document, is 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

## Guidance

This guidance supports police forces and all organisations accessing PNC or LEDS in meeting the aims of the Code.

The Code also reflects data protection and human rights legislation, and considers the seven principles of public life (‘Nolan Principles’) and the **Code of Ethics for policing**. The Code has been written to be consistent with the data protection principles. This guidance should therefore be read together with any relevant Information Commissioner’s Office (ICO) guidance on general and law enforcement processing.

## Aims of the Code

The objective of the Code, taken together with this guidance document, is to provide public confidence in the legitimacy and integrity of information that is supplied through PNC or LEDS and

the lawful purposes for which this is applied.

The stated aims of the Code are as follows.

## Safeguarding people

Facilitating the appropriate use of accurate data by 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 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 both system users and the wider public can be confident in understanding how personal 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 protect their data and privacy interests.

## Enabling performance

Continuously 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 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 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 (and this guidance) support the mechanisms (training, learning, management, audit and inspection) that will ensure that personal data is not used in a discriminatory manner or unethical manner. The Code will be reviewed regularly so it is consistent with evolving human rights, data protection and ethical standards, such as the Code of Ethics for policing. The College of Policing has developed the **Police Race Action Plan** jointly with the National Police Chiefs' Council (NPCC) and it is essential to eliminate any racial bias, stereotyping, profiling or discrimination in the use of personal data.

## Benefits of high quality data sharing

Using data for law enforcement will only be effective if that data is of high quality.

- **Read further detail on how 'high quality' is defined**

Applying the Code, together with this guidance, should ensure that a high level of data quality is maintained, and encourage better use of data for appropriate purposes.

The ability of forces to quickly share high-quality data ensures that there is a greater chance of identifying patterns of behaviour, whether this be serial perpetrators of violence, or people who are identified as vulnerable. This is relevant when crimes are committed across multiple force boundaries (for example, county lines).

Sharing access to accurate data nationally helps policing, law enforcement and safeguarding agencies understand the true nature of the challenges they face, while ensuring the safe, effective and efficient deployment of resources. This results in public benefits through public protection, crime investigation and multiagency safeguarding, as policing can become 'borderless.

Examples of borderless policing include the following.

- Police may search for crimes across county borders.
- An arresting force can find the relevant offending history of an individual throughout the United Kingdom. For example, where a person is arrested for stalking and harassment offences, data

from other forces will identify if this person has any previous history of similar offending and if this offending is part of a picture of escalation.
- Data on high-risk offenders shared with probation officers can improve the management of risk when individuals are returned to their communities or move to another location.
- Police forces can share data with schools at the earliest opportunity to alert them of children who have been exposed to domestic abuse or other forms of adverse childhood experience.

# Scope of the Code and guidance

The Code applies directly to every chief officer (as defined in section 101(1) of the Police Act 1996) of a police force in England and Wales who has access to PNC and LEDS in connection with the discharge of their functions, that is, the chief officers of those police force areas in England and Wales that are subject to section 39A of the **Police Act 1996**.

Legally, every chief officer must have regard to the Code in discharging any function relating to the management and use of both PNC and LEDS, as well as the data that is entered and processed for use as law enforcement information.

## Other organisations

PNC is already used by other organisations and LEDS will be, so the Code should be applied by other law enforcement agencies who access and use information through either system. It will be adopted by other police forces within the United Kingdom (Police Scotland, Police Service of Northern Ireland and those in other local jurisdictions), as well as law enforcement agencies or other agencies who may access PNC or LEDS and selected data sets.

Some organisations connect through an arrangement with ACRO Criminal Record Office (ACRO). All user organisations that have been granted access to the platforms and selected data sets (directly via an interface or indirectly via ACRO) will be required to commit in writing to follow the standards as set out in the Code, and to comply with the supporting responsibilities and obligations set out in the relevant sections of this guidance, together with the security arrangements for each system. Consideration has been given to what extent the scope of the code extends to organisations which receive data extracts, which include personal data. The joint controllers recommend and encourage these organisations to pay attention to the best practice principles of the Code and this will be included in their data sharing agreements.

A list of the current organisations that are signing up to the use of PNC and LEDS will be maintained by the Home Office, on behalf of the joint controllers. Part 3 of the Data Protection Act (DPA) 2018 identifies the bodies (including those also known as **competent authorities**) that are likely to be processing data for law enforcement purposes as including:

- the police
- criminal courts
- prisons
- non-policing law enforcement
- any other body that has statutory functions to exercise public authority or public powers for law enforcement purposes

## Exemptions to the application of the Code

There are certain exemptions to the application of the Code. For example, courts acting in their judicial capacity, and regulatory bodies accessing data to oversee data controllers would not be covered.

Judicial office holders can apply the Code in their determinations but are not bound by it. However, courts acting in administration of justice – for example, communicating court results – are bound by the Code, when they sign up to user agreements working through the Ministry of Justice as users and suppliers of data into, and from, PNC and LEDS.

Regulatory bodies, such as the ICO, may access PNC and LEDS in carrying out their regulatory duties and will be compliant with data protection legislation but not subject to this Code.

It is also envisaged that there may be rare occasions when emergency services would access data to provide emergency care where they cannot obtain that person’s consent.

## Responsibility for compliance

The Code defines who is responsible for organisational and user compliance.

For policing, the Code applies directly to the chief constable., including the Commissioner of Police of the Metropolis and the Commissioner of the City of London Police.

Where other organisations are granted access to PNC and LEDS, they will be required to sign up to the Code through **the contracting arrangements**. Chief officer responsibility then extends to those named individuals with responsibility for senior management. This may be chief officers of other police forces, such as Police Scotland or the Ministry of Defence Police, or it may be the chief executive officers, chief executives, directors and permanent secretaries of those organisations. Those individuals will also be held responsible for organisational and user compliance with the guidance.

# Policing, law enforcement and safeguarding purposes

The Code applies to all data processed through either PNC or LEDS. It concerns the processing of data for legitimate purposes, primarily law enforcement, but also wider policing, safeguarding and national security purposes. These purposes are defined below.

Everyone in law enforcement and policing must maintain legal, ethical and professional standards in using data and personal information for legitimate purposes. These legitimate purposes are defined below as policing, law enforcement and safeguarding purposes.

## Policing purposes

The original definition of policing purposes came from the Code of Practice on the Management of Police Information 2005 (now replaced by the **Police Information and Records Management Code of Practice 2023**) and still remains in place. Policing purposes are 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

## Law enforcement purposes

Under section 31 of the DPA 2018, law enforcement purposes are specifically defined as the following.

> *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.*

The term ‘law enforcement purposes’ encompasses most policing purposes as defined above, which are covered by Part 3 of the DPA 2018. If the policing purpose falls outside the definition of law enforcement purposes – for example, in providing educational programmes or supporting communities – processing will be governed by the UK GDPR.

Law enforcement bodies may also occasionally process some PNC data for general purposes, such as human resources, when reviewing an individual’s access for performance or disciplinary reasons. PNC and LEDS will be accessed by policing and also wider law enforcement bodies and other partner agencies, who are subject to Part 3 of the DPA 2018 if processing data for a law enforcement purpose.

## Safeguarding purposes

Safeguarding is a widely accepted 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. The term ‘safeguarding purposes’ in the Code reflects the work of police and other agencies in protecting the health, wellbeing and human rights of individuals at risk.

Although subject to the UK GDPR, ‘safeguarding purposes’ are not specifically included in the definition in section 31 of the DPA 2018, although they are increasingly part of wider law enforcement activity.

## Tags

Information management