College of Policing

college.police.uk

Code of Practice for the Law Enforcement Data Service (LEDS)

Consultation

June 2020

The Code of Practice for the Law Enforcement Data Service (LEDS) will be presented to Parliament pursuant to Section 39A (5) of the Police Act 1996, as amended by Section 124 of the Anti-social Behaviour, Crime and Policing Act 2014

Any enquiries regarding this publication or to request copies in accessible formats please contact us at **contactus@college.pnn.police.uk**

Contents

1 Introduction

1.1 The Code of Practice for the Law Enforcement Data Service (LEDS) is issued by the College of Policing, under Section 39A of the Police Act 1996. It serves as statutory guidance for the police forces of England and Wales. Every chief officer of police should have regard to the code in discharging any function to which this Code of Practice ("the Code") relates.

1.2 This Code of Practice 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 LEDS is governed, managed and used. A detailed supplement to this Code of Practice, the Guidance Document, has been created to provide more detail on how managers and users within organisations which sign up to access LEDS can support their chief officers in complying with the requirements of the Code. This also clarifies some responsibilities for the Home Office as system owner.

1.3 As a code of practice, the Code may be taken into account in a court of law and in disciplinary proceedings. The Code makes reference to specific legal requirements and any breaches of these should be treated in accordance with that legislation. The Code will be considered by a number of bodies which may seek to hold users to account for data management practice in a law enforcement or safeguarding context, for example the Information Commissioner's Office (ICO), or the Independent Office for Police Conduct. In particular, 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.

1.4 The existing Codes of Practice for the Police National Computer (PNC) and Police National Database (PND) will work in parallel with this Code, until these systems have been decommissioned. If information is being accessed through LEDS, organisations and individuals will be expected to comply with the LEDS Code of Practice, and the legislation referenced within the Code. The Codes of Practice for the PNC and PND are supplemented by 'The PNC User Manual' and 'The Police National Database (PND) Manual of Guidance/Business Rules' respectively. These documents will also be referenced as guidance for LEDS until such time as a LEDS user manual and set of business rules replace them.

2 The purpose of the Code

2.1 The purpose of the Code is to support the ethical, fair and diligent use of LEDS. The Code supports key principles in upholding fundamental human rights, demonstrating respect to all people and acting in accordance with the law. The Code is underpinned by the seven principles of public life ('**Nolan Principles**'), the **Code of Ethics** for Policing and the principles set out in data protection legislation.

2.2 The Code seeks to provide public confidence in the legitimacy and integrity of how data is processed in LEDS through five important aims:

Safeguarding people: Facilitating the appropriate use of accurate data by law enforcement agencies to bring offenders to justice, prevent crime and protect vulnerable people. LEDS will also include the National Register of Missing Persons (NRMP) to help agencies locate those who are missing and safeguard people who may be vulnerable.

Promoting accountability: Ensuring that activities undertaken in relation to LEDS have clear lines of responsibility, so each organisation that uses or supplies data can demonstrate that they understand and comply with the principles that support the Code. The Code and the Guidance Document encourage transparency in how personal data within LEDS is used, managed and deleted.

Promoting understanding: Enabling greater understanding of the objectives of LEDS as a law enforcement information system. The Code and Guidance Document use plain language so users of LEDS can be confident in how to use the system to support the prevention and detection of crime, protect the public and safeguard vulnerable people. Members of the public should feel reassured that the protections provided by the Code and the Guidance Document will help to preserve their data and privacy interests.

Enabling performance: Continuously improving the value of the data within 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 in the use of LEDS and a requirement for organisations to proactively support continuing practice development among all users.

Promoting fairness: The public need confidence in the integrity of data processing within LEDS and have faith that it is compliant with the law. The processing of personal data for law enforcement purposes must be lawful, fair, transparent, and consistent with data protection principles. Information created and retained by law enforcement must be proportionate, lawful, ethical and necessary. The Code and Guidance Document support the mechanisms (training, learning, development, audit and inspection) that will ensure LEDS is not used in a discriminatory or unethical manner. The Code and Guidance Document will be reviewed regularly to make sure they are consistent with evolving human rights, data protection and ethical standards, such as the **Code of Ethics** for policing.

2.3 Everyone in law enforcement and policing must maintain lawful, ethical and professional standards when using data and personal information for law enforcement safeguarding and wider policing purposes. This is crucial in ensuring public confidence in the legitimacy and integrity of how such data is collected, maintained, applied and eventually deleted.

2.4 **Article 8** of the Human Rights Act 1998 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 justified. Interferences with privacy will include using personal data where it is either not necessary or not proportionate. In some instances, failure to use data or share data appropriately could also be considered an interference with an individual's 'private and family life'. All rights enshrined in human rights legislation should be considered by LEDS users so that decisions made in processing data within and from LEDS are legal, ethical, proportionate and balanced. By doing so, the public can have confidence in the way police and other organisations that use LEDS are accessing and managing the system.

3 Statutory basis of the Code

3.1 The College of Policing issues this Code as statutory guidance under the **Police Act 1996**, s 39 A, as amended by the **Anti-Social Behaviour, Crime and Policing Act 2014, s 124**.

3.2 As a code issued under that legislation, the legal status of the Code of Practice for LEDS:

- applies to the police forces maintained for the police areas of England and Wales, as defined in the **Police Act 1996**, s 1 (or as defined in any subsequent legislation)
- relates specifically to chief officers in the discharge of their functions. A chief officer of police shall have regard to the Code

3.3 The legislation provides that chief officers of the following organisations are primarily responsible for organisational compliance with the Code. This includes:

- the chief constable, in relation to a police force maintained under the **Police Act 1996**, s 2
- 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 City of London Police
- the chief constable, in relation to the British Transport Police

3.4 This Code should be read in conjunction with the associated Guidance Document. The Guidance Document details the requirements which support the 10 principles of the Code and user organisations are required to ensure organisational compliance with that guidance. The Guidance Document also clarifies how managers of LEDS user organisations and staff who are direct users have responsibilities to support their chief officers in relation to the Code. This also ascribes responsibilities to both the Home Office and the National Police Chiefs' Council (NPCC) in relation to the strategic oversight of access to LEDS, its operational use by police (and other organisations), and application of data sourced through LEDS. The Guidance Document also provides useful background information and references to other guidance or reference material, which should be followed.

3.5 The Code recognises that there is an existing legal framework for the use of information in legislation relating to data protection and human rights. This should be followed by all chief officers, LEDS users and their managers. Everyone

who has access to personal data is required to use it according to the current legislative framework. The Guidance Document references current legislation, such as the **DPA 2018** and the **Human Rights Act 1998**. The Guidance Document provides further detail and direction on how the legal framework operates. Such legislation may change and it is the responsibility of all organisations to ensure that LEDS users operate at all times in accordance with legislation and this code.

3.6 Data protection legislation identifies certain organisational responsibilities in the processing of data. LEDS user organisations will be subject to joint controller arrangements which take account of the different types and sources of data, the different purposes of the processing and the status of organisations in terms of the data protection legislation. Those arrangements will necessarily reflect those differences.

3.7 The Home Office and the NPCC will have significant responsibilities as lead joint controllers for LEDS. The Home Office has primary responsibility for the LEDS IT system and for some of the data sets held on LEDS. The NPCC acts as a coordinating body for chief officers of police across the United Kingdom through an agreement made under s **22A of the Police Act 1996** and has a role in providing leadership and direction to police forces in the United Kingdom who will use LEDS. Although all chief officers are joint controllers for their forces, that coordination role of the NPCC is important. LEDS will be subject to a Joint Controller Agreement (JCA) setting out the arrangements for policing joint controllers.

4 Scope of the Code

4.1 This Code and the Guidance Document should be considered by organisations other than police forces in England and Wales. By contractual arrangements, it will be applicable to other agencies within the United Kingdom that can access LEDS and selected data sets. This includes police forces that are not covered by the **Police Act 1996, s 1**, as well as other agencies with access to LEDS that exchange information with the police service in England and Wales.

4.2 All LEDS user organisations, through their respective chief officer/chief executive representatives, will be required to commit in writing to follow the Code. This means that law enforcement and safeguarding agencies using LEDS should take account of the Code and the Guidance Document, and will be required to comply with monitoring arrangements, which include potential inspection by HMICFRS. This includes some commercial organisations which may access LEDS under data-sharing with access limited to redacted or filtered data for use in applications which support law enforcement purposes, such as checking for vehicle fraud.

4.3 While chief officers may delegate the execution of those responsibilities to senior managers, such as the Senior Information Risk Owner (SIRO), they will be held to account for any failures by the organisation in respect of compliance with the Code and relevant legislation.

5 Policing, law enforcement and safeguarding purposes

5.1 This Code concerns the use of LEDS for law enforcement, other policing or safeguarding purposes.

5.2 Law enforcement purposes are defined for the purposes of this Code as:

> **'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 Policing purpose may fall outside the definition of the law enforcement purposes (for example in providing educational programmes or supporting local communities). The Guidance Document provides further information on how data processing of personal information for law enforcement and policing is treated under current data protection legislation.

5.5 The Code also addresses more extensive applications of LEDS 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. The Guidance Document provides further information on how data processing of personal information for safeguarding activities are treated under current data protection legislation.

5.6 Further, processing of personal data collected for the law enforcement purpose is permitted if that processing is authorised by law, and the processing is necessary and proportionate to that other purpose. Personal data collected for the law enforcement purpose should not be processed for a non-law enforcement purpose (including other policing or safeguarding) unless it is authorised by law.

6 Ten principles for the ethical and professional use of LEDS

6.1 Securing the data held on LEDS

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 information on LEDS.

6.2 Creating the data record on LEDS

Data stored on LEDS should only be created or entered for law enforcement, other policing or safeguarding purposes, and must be of high quality.

6.3 Amending and updating the data record on LEDS

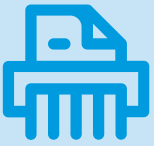
Police or law enforcement information must be accurate and up to date while it is being used by agencies who require it to discharge their law enforcement, other policing and safeguarding responsibilities. This requires that the data set is proactively reviewed and updated for accuracy and currency.

6.4 Validating the data record on LEDS

The data available on LEDS must be correct and relevant. This involves validating or checking LEDS (or originating 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 on LEDS

Data held on LEDS must be regularly reviewed to make informed decisions on retention and deletion of that data, particularly personal data, that comply with all legal and policy requirements and to protect the integrity of the data.



6.6

Accessing and applying the data held on LEDS

LEDS information and data should be used ethically and in accordance with human rights and equality legislation.

6.7

Reporting and analysing the data held on LEDS

Data obtained from LEDS should 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 held on LEDS

Data from LEDS must be processed lawfully and ethically. Shared access to data is essential to discharging law enforcement, other policing or safeguarding purposes and this Code seeks to encourage effective data disclosure to better support law enforcement and public protection.

6.9

Accountability for and auditing of LEDS data access and usage

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

6.10

Training and continuing professional development for LEDS

Training in using LEDS effectively will ensure system integrity, better protection of data subjects' rights and better outcomes for law enforcement.

7 Compliance and malpractice

7.1 This Code is statutory guidance. It may be taken into account in a court of law and in disciplinary proceedings. It is the responsibility of the chief officer to ensure that all personnel who have access, or may be in a position to gain access to LEDS, are fully aware of the Code and the potential consequences of a breach of the Code. Responsibility for the compliance of police forces is vested in chief officers by the **Police Act 1996**.

7.2 The Guidance Document makes reference 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.

7.3 National arrangements for whistleblowing will be put in place to protect those who express concerns about malpractice and the existence of the local whistleblowing arrangements will be part of the LEDS inspection regime. As a condition of access to LEDS, HMICFRS will also have powers to inspect other law enforcement organisations that have access to LEDS. Other bodies, such as the Biometrics Commissioner or the Independent Office for Police Conduct, will also have an interest in how this Code is applied.

7.4 Individuals whose data may be contained within LEDS, or concerned parties who believe that there may be evidence of breach of the Code, should report those concerns to the Home Office.

7.5 The Home Office working with the NPCC and College of Policing will support an annual review and refresh of the Code and Guidance Document until such time as LEDS becomes fully functioning and then regularly thereafter. This will take into account changes in the function and use of LEDS as it advances, changes to legislation and guidance which support that use and changes to the application of data held within LEDS. This will include a formal consultation process.

About the College

We're the professional body for everyone who works for the police service in England and Wales. Our purpose is to provide those working in policing with the skills and knowledge necessary to prevent crime, protect the public and secure public trust.

college.police.uk

Follow us
@CollegeofPolice

C066I0520