College of Policing

college.police.uk

Code of Practice for Law Enforcement Data Service (LEDS)

Guidance Document

Subtitle (*Date to be determined*)

Version 0.4 1(Draft for Consultation)

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

CONTENTS

A CODE OF PRACTICE FOR THE LAW ENFORCEMENT DATA SERVICE

1 INTRODUCTION

1.1

This Guidance document provides a background for the Code of Practice for the Law Enforcement Data Service (LEDS) ("the Code") but does not form part of the Code itself. The Code of Practice is contained within a separate document, which should be read in conjunction with this document. *This version of the guidance document is a draft which will be subject to consultation, including a formal public consultation, before being laid before Parliament, by December 2020.*

1.2

The Home Office, through the National Law Enforcement Data Programme (NLEDP), has created a national Law Enforcement Data Service (LEDS) which provides Police and other Law Enforcement agencies, with on-demand, at the point of need, current and joined up information in order to prevent crime and better safeguard the public. This work will in due course result in the decommissioning of the Police National Computer and Police National Database. The National Law Enforcement Data Programme (NLEDP) is relocating and combining the separate PNC and PND systems onto a single technology platform in LEDS. The LEDS platform allows a single interface for a number of existing data sets which facilitate the use of PNC and PND for law enforcement. A National Register of Missing Persons will be located within LEDS and the structure of the platform will allow addition of further data sets at a later date.

1.3

The data sets from both PND and PNC will co-locate onto LEDS to improve accessibility for those users that need full access to both, whilst security provision will be in place to retain separation for those users that only need access to specific data sets. This interoperability will provide law enforcement agencies with an enhanced set of national information accessible through a single route for the first time.

1.4

Working alongside the NLEDP, the College of Policing has developed the Code of Practice to cover all aspects of the behaviours and use of LEDS and provide 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 being governed, managed and used. This Code of Practice is intended to provide a robust document with which to hold all LEDS user organisations to account. The existing Codes of Practice for PNC and PND will work in parallel until these systems have been decommissioned, however if information is being accessed through LEDS, organisations and individuals will be expected to comply with the LEDS Code of Practice. The Codes of Practice for 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 replaces them.

1.5

This document is addressed to those who are responsible for developing, maintaining and securing the integrity of LEDS as an information platform. It is also addressed to all organisations who are granted access to the platforms, their managers, members and staff, and those who will be responsible for training for implementation and use of LEDS. A separate Public Guide to the Code of Practice for LEDS assists members of the public, those whose data may be held on LEDS and those interested in the scrutiny of LEDS as a law enforcement asset, with guidance as to how data could be used within LEDS, and also how to get access to, change or delete personal information wrongly entered or retained. Included in the Public Guide are links to a list of the organisations which currently are permitted to access LEDS.

1.6

Everyone in law enforcement and the police service, in particular, must maintain high ethical and professional standards when using data and personal information for law enforcement and safeguarding purposes. This is crucial in ensuring public confidence in the legitimacy and integrity of how such data is collected, maintained and applied.

1.6

The College of Policing, working with the Home Office and on behalf of the National Police Chiefs Council, seeks to enable this confidence by;

a) Creating the Code of Practice for LEDS in sufficient detail such that users, managers, suppliers, auditors, trainers etc. will be able to determine what their responsibilities are and understand whether they have been met

b) Maintaining the Code of Practice and the Public Guide in a single online publicly available place. Included in that public space will be the answers to frequently asked questions

c) Reviewing and refreshing the Code of Practice and Public Guide regularly to take account of new developments or thinking.

2 STATUTORY BASIS OF THE CODE

2.1

The College of Policing *will issue* the Code of Practice for LEDS as a code of practice under section 39A of the Police Act 1996 (as amended by section 124 of the Anti-Social Behaviour, Crime and Policing Act 2014).

2.2

As a code of practice, the legal status of the Code of Practice for LEDS:

a) applies to the police forces maintained for the police areas of England and Wales as defined in section 1 of the Police Act 1996 (or as defined in any subsequent legislation)

b) relates specifically to chief officers in the discharge of their functions. A chief officer of police shall have regard to this code, as will the members of the police force for whom the chief officer of police is responsible.

2.3

This code recognises that there is an existing legal framework for the use of information in legislation relating to data protection and human rights, and references pertinent legislation, such as the Data Protection Act 2018 (DPA) and the Human Rights Act 1998. In particular Part 3 of the DPA sets out a specific regime for law enforcement authorities.

3 SCOPE OF THE CODE

3.1

The scope of the Code of Practice for LEDS extends beyond its statutory basis as a code of practice for police forces in England and Wales. It is applicable to other agencies, including other police forces not covered by section 1 of the Police Act 1996 and law enforcement agencies within the United Kingdom (England, Wales, Scotland, Northern Ireland, the Isle of Man and the Bailiwicks of Jersey and Guernsey) that exchange information with the Police

Service in England and Wales, and have been granted access to LEDS, under data sharing agreements. Primary responsibility for organisational and user compliance with the Code will therefore vest in chief officers, which includes:

i) in relation to a police force maintained under section 2 of the Police Act 1996, the Chief Constable

ii) in relation to the Metropolitan police force, the Commissioner of Police of the Metropolis

iii) in relation to the City of London police force, the Commissioner of Police for the City of London

iv) in relation to the British Transport Police, the Chief Constable, and

v) in the case of other organisations using LEDS, their equivalents (Chief Executive Officers, Chief Executives, Directors, Permanent Secretaries, and other individuals with senior responsibility for managing the organisation)

3.2

A “LEDS User” is an individual who has been vetted and approved to log in to the service and trained to access the functionality. They will either be registered as a direct user or will be a member of an organisation which has been granted access through a connecting system. Chief officers must introduce and maintain vetting and accreditation arrangements within their organisations, in accordance with police or Government vetting standards, so that the operation and use of LEDS complies with the principles set out in the Code and with guidance issued under this code or referenced within the code. Unless otherwise stated, “use of LEDS” includes any data functions associated with the platform, including accessing the platform, and using the information obtained from the platform. A “LEDS user” may have a specific designated role such as data entry, or could be a frontline Police Officer accessing LEDS for operational reasons. Therefore some of the responsibilities which apply will be role specific not generic.

3.3

The expectation of the public is that every organisation that will access and use LEDS will comply with the responsibilities and obligations set out in the Code of Practice for LEDS. The Home Office will not have statutory responsibility for many of these bodies but works in collaboration with the National Police Chiefs Council (NPCC) and other designated Joint Controllers of the service (under the provision of the Data Protection Act 2018). The NPCC acts as a co-ordinating body for police forces across the United Kingdom through an agreement made under Section 22A of the Police Act 1996. All LEDS user organisations will

be required to sign up to a data sharing agreement issued on behalf of the Joint Controllers, which will stipulate that adherence to the Code is mandatory. It is also an expectation that suppliers of services will also adhere to the expectations of the Code including its Data Protection Act obligations in ensuring that the systems which will connect with LEDS facilitate all requirements.

3.4

A full list of the current organisations which are signing up to the use of LEDS will be maintained by the Home Office and will be available online. Part 3 of the Data Protection Act (DPA) 2018 defines the competent authorities processing data for law enforcement purposes as, but not limited, to:

a) the police, criminal courts, prisons, non-policing law enforcement; and

b) any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

Data on LEDS may also be shared for safeguarding vulnerable children and adults, particularly data held within the National Missing Person's Register. LEDS data may also be accessed by some commercial organisations under data sharing agreements but access is limited to applications which support policing and law enforcement purposes, such as checking for vehicle fraud.

4 THE PURPOSE OF THE CODE OF PRACTICE

4.1

The purpose of the Code is to support the ethical, fair, diligent and impartial use of the LEDS platform. The Code supports key principles in upholding fundamental human rights, demonstrating equal respect to all people, and acting in accordance with the law. In particular, the 7 principles of public life ('Nolan Principles'), the Code of Ethics for Policing and the Law Enforcement Principles set out in the Data Protection Act 2018, underpin the Code. The Code will achieve this through 5 equally important aims:-

a) **Safeguarding people**: - Facilitating the use of data by law enforcement and other agencies at the appropriate time and in the appropriate way. Using accurate and joined-up information in order to bring offenders to justice, to prevent crime, protect the public and better safeguard the vulnerable. This Code of Practice will facilitate digital collaboration between different law enforcement organisations, the criminal justice sector and other partners in a more efficient and effective way.

b) **Promoting accountability**: - Ensuring activities undertaken in relation to LEDS have clear lines of responsibility. Each organisation, their managers and individual users, need to recognise and acknowledge these responsibilities so that they can demonstrate that they comply with the principles underlying the Code.

c) **Promoting Understanding**: - Enabling greater understanding of the objectives of LEDS as a law enforcement information platform. The Code uses plain language to enable the users of LEDS to be confident in the activities they need to undertake to prevent and detect crime and safeguard the vulnerable. This also allows the public reader to be confident of the protections in place to preserve their data and privacy interests.

d) **Enabling Performance**: - Supporting performance through a quality management regime, which delivers continuous improvements to the value of the information within LEDS including; promoting better data quality, ensuring the relevance of the information and strengthening the partnership working where information is shared across organisational boundaries. This will be facilitated by training to support implementation and a requirement for organisations to pro-actively support continuous practice development and improvement amongst all users.

e) **Promoting Fairness**: - Reinforcing the mechanisms (training, learning, development, audit and inspection) that will ensure that LEDS is not used in a way that is discriminatory or otherwise unfair to anyone based on their age, race, ethnicity, any faith or belief, gender, gender identity, sexual orientation or any disability. Ensuring the Code is reviewed against, and maintained consistent with, evolving Human Rights, Data Protection and Ethical Standards, such as the principles enshrined in the Government's Data Ethics Framework which guides the design of appropriate data use in government and the wider public sector. The Code will adhere to relevant data protection legislation and underline Management of Police Information (MoPI) and other principles, to advocate that the amount of information retained by law enforcement is constrained by what is considered fair, legal, proportionate and necessary.

5 DEFINITIONS

5.1 DATA PROTECTION AND DATA PROCESSING

a) Data protection is concerned with the fair and responsible use of personal data. For these purposes, data is information that has been translated into a form that is efficient for movement or processing. References to data in the Code include police and law

enforcement information. All information, including intelligence and personal data obtained and placed on LEDS is referred to as data throughout the Code.

b) The UK data protection regime is set out in the Data Protection Act (DPA), 2018, along with the General Data Protection Regulations (GDPR) which form part of UK law. It takes a flexible risk-based approach, which puts the onus on organisations to consider and justify how and why it uses data. Processing under the Act is the activity that personal data is subjected to, creation, storage and sharing and other activities. This includes data processed for law enforcement purposes (see below). The Information Commissioner's Office (ICO) regulates data protection in the UK. This Code of Practice is intended to support and not supersede the powers of the ICO, in relation to law enforcement processing.

c) Under the provisions of the DPA 2018 there has to be a controller. This is the person within the organisation who determines the purpose and means by which the processing of personal data occurs. Within the police service, the controller is the chief officer. Each chief officer of an organisation which supplies data to LEDS, is individually responsible for the personal information held in data within those organisational systems which feed LEDS. Under arrangement with the NPCC those individuals are also then jointly data controllers for the data held in LEDS. Organisations which process personal data from LEDS (which can include accessing the data set) do so with the permission of the joint data controllers. These permissions will be set out in a data sharing agreement. The Home Office will issue each agreement on behalf of the joint controllers.

d) Part 3, Chapter 3 of the Act provides the following individual rights: 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. Certain rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. Further, there are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights. For example, subject access rights and the rights to rectification, erasure and restriction do not apply to the processing of 'relevant personal data' in the course of a criminal investigation or criminal proceedings.

5.2 Data Processing Functions

Data processing is, broadly speaking, the collection, storage and manipulation of items of data to produce meaningful information. Data processing for LEDS may involve various

processes or functions, including creating the data record, amending the data record, validating data, reviewing, retaining and deleting data, accessing and applying data, sharing data, analysing data and auditing data. These functions have been broken down within the Code of Practice and assigned responsibilities or obligations that describe the good practice for data processing for LEDS. Other supporting functions, such as training for LEDS and securing the data on LEDS have been similarly described. Maintaining integrity and quality assurance of the service are 'golden threads' which run through the Code.

5.3 Policing, Law Enforcement and Safeguarding Purposes

a) Policing purposes are defined in Code of Practice on The Management of Police Information 2005 as:

(1) protecting life and property,

(2) preserving order,

(3) preventing the commission of offences,

(4) bringing offenders to justice, and

(5) any duty or responsibility of the police arising from common or statute law.

b) Law Enforcement purposes are defined under section 31 of the DPA 2018 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."

c) The Code addresses both policing, wider law enforcement bodies and other partner agencies using LEDS. For the purposes of clarity, the term ***law enforcement purposes*** is used to encompass the policing purposes as defined above and the Code also addresses wider ***safeguarding purposes*** in protecting children and vulnerable adults from harm, which are not included in section 31 DPA 2018.

6. Guidance

6.1

Reference has been made in the Code to specific pieces of legislation and guidance, which inform best practice in data processing and the use of LEDS. Guidance on expected performance and practice is issued to police forces from time to time by relevant bodies, such as the National Police Chiefs' Council (NPCC) which succeeded the Association of

Chief Police Officers (ACPO) on April 1 2015, and took over ownership of ACPO guidance, which remains current. The College of Policing, the professional body for policing since 2012, is mandated to set standards in professional development, including codes of practice and regulations, for the 43 forces in England and Wales. The College of Policing produces Authorised Professional Practice (APP) which provides further detail to support expectations of good practice. Whilst this in itself does not have statutory mandate, its inclusion within the Code should be considered as a further indication of the standards of practice and performance to be expected of LEDS users. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) will apply the same standards to all organisations accessing LEDS and will use guidance such as APP as the benchmark of good practice. Whilst written to support policing, wider law enforcement agencies should access APP and should incorporate that guidance into their own context.

The APP website can be accessed from any internet enabled device. It is available at www.app.college.police.uk.

7 GOVERNANCE OF LEDS

7.1

At the time of writing the exact structure for governance of LEDS is still under discussion. For the purposes of this Code of Practice, a level of responsibilities has been ascribed to both the Home Office, as platform owner and the National Police Chiefs' Council (NPCC) on behalf of the joint controllers. Whichever organisation/body becomes the LEDS sustainment organisation will be led by a nominated lead from the NPCC.

7.2

The Home Office, as platform owner, holds responsibilities for implementation of LEDS in conjunction with the joint controllers. For the purposes of the Code the Home Office and NPCC hold responsibilities in relation to governance of LEDS and in providing leadership and direction to the law enforcement agencies who will access LEDS and the data within it. As described in the Code organisations will be required to ensure that managers and users of LEDS are fully supported to undertake appropriate training, learning and development for the use of the platform and data. The College of Policing and the Home Office will develop the framework and mechanisms through which this can occur.

7.3

The Home Office will apply the Government and Information Risk Review (GIRR) process to formalise the connections between LEDS with other information systems which it will

exchange information. This will provide a level of assurance on both technical and procedural requirements. Chief Officers and Chief Executive Officers who seek to use LEDS, will be required to consider the fitness for purpose of their own supply systems and the implications of contractual relationships with vendors of those systems. The Home Office will work with Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) and chief officers of user organisations, to provide an annual assessment of how their internal systems are working and how their suppliers are meeting obligations. Supplier systems that are not deemed suitable may not be approved to connect to LEDS, or may have connection withdrawn at a later date.

8 COMPLIANCE AND MALPRACTICE

8.1

The Code of Practice is statutory guidance which will be admissible in a court of law and in disciplinary proceedings. The Code will make reference to specific legal requirements and any breaches of these should be treated in accordance with that legislation. Failing to otherwise comply with the Code may not in itself cause an organisation or individual person to be prosecuted. However the Code, in whole or part, can be used in evidence in any court proceedings.

8.2

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) will use the Code, associated guidance, and standards to monitor and hold organisations who access LEDS to account. HMICFRS will also have powers to inspect other law enforcement organisations accessing LEDS as a condition of data sharing agreements. Other bodies as appropriate (such as the Information Commissioner's Office, and Biometrics Commissioner) will seek to understand how effective this Code of Practice has been in promoting compliance with data protection legislation and data quality expectations.

8.3

Individuals whose data may be contained within LEDS, or concerned parties who believe that there may be evidence of breach of the Code of Practice should in the first instance report those concerns to the Home Office, as the governance body for LEDS. Details of the mechanism for reporting concerns are outlined in the Public Guide to the Code of Practice for LEDS.