

National Law Enforcement Data Programme:

LEDS: Code of Practice

Discussion Document

20 September 2018

This Document has been written with the aim of stimulating discussion on the Code of Practice for LEDS. It is not intended to be viewed as current Home Office policy or intention. It is to be circulated to Law Enforcement Governance bodies and Civil Society Organisations for reflection.

NLEDP – Non-Paper

1. This paper has been written to stimulate a discussion prior to the drafting of a Code of Practice (Code) for the combined Law Enforcement Data Service (LEDS). LEDS will replace the Police National Computer (PNC) and Police National Database (PND) and therefore the existing PNC and PND Codes of practice will be replaced. The LEDS Code, like the existing PNC and PND Codes, will be statutory guidance; a Parliamentary Code under Section 39A of the 1996 Police Act. The purpose of this document is to define the questions the LEDS Code of practice will be commissioned to answer.
2. This paper will start with the high-level principles behind the requirement to write a new Code, will extract some of the previous relevant learnings, describe some of the topics the Code will need to cover and propose a candidate purpose for the Code. This document, specifically the purpose statement will be used to task the Code authors.

Is the proposed purpose statement satisfactory? What further measures need to sit underneath the purpose statement?

3. The existing PNC Code was written in 2004 and has been described by the Her Majesty's Inspector of Constabulary Fire and Rescue Services "...as seriously out of date...".¹ The purpose of the existing PNC and PND Codes are in appendix A and B respectively. The PND Code dates from 2010 and whilst it is more up to date it still needs to be re-written in order to meet the expected way in which LEDS will work.
4. It is proposed the LEDS Code therefore needs to meet the following principles;
 - a. Modernised to take account of current thinking on relevant Codes,
 - b. Take into account changes in legislation and regulation
 - c. More inclusive of the behavioural standards required for LEDS, and
 - d. Comprehensive and easy to read for the different audiences that might read it.

Human Rights

5. In 2008 the Government lost a European Court of Human Rights (the Court) Case in relation to otherwise lawful activity.² This was principally because the Code of Practice covering Lawful Interception was insufficiently clear. The Court accepted the argument that in "...accordance with the law..." means

¹ <https://www.justiceinspectors.gov.uk/hmicfrs/wp-content/uploads/police-national-computer-use-acro-criminal-records-office.pdf> (Page 3)

² Liberty & Others v United Kingdom 2008 European Court of Human Rights 58243/00 [1 Jul 2008]

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

NLEDP – Non-Paper

having a basis in domestic law and, in this context being accessible to an individual who might be affected by the practice and enabling that individual to foresee the consequences for them (even if it must be explained). The rulings were that;

Accessibility and foreseeability weren't met

6. The Court ruled there was insufficient detail and precision to meet the foreseeability requirement and that foreseeability could be better achieved if those affected were made aware of the impacts. Further the Court suggested the domestic law must be sufficiently clear "...to give citizens an adequate indication as to the circumstances in which...public authorities are empowered to resort to any such measures." The Court ruled this must go beyond merely noting the existence of existing procedures, and that a Code must go further in terms of adding additional clarity. The Court outlined that accessibility and foreseeability would be satisfied by the knowledge of the criteria (used to satisfy the selection and deletion of data) and knowledge of the existence of the multiple safeguards that had been established.

Insufficient protections against arbitrary interference

7. The Court ruled in relation to arbitrary interference that as surveillance was not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for any legal discretion granted to be expressed in terms of an unfettered power. Therefore, the law must indicate how the competent authorities exercise any discretion with sufficient clarity to give the individual adequate protection against arbitrary interference.

Insufficient clarity over the procedure

8. The Court found the Code should identify the nature of the offences which may give rise to the activity; a definition of the categories of people liable to be subject to the activity; a limit on the duration of the activity; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data may or must be erased.
9. To deal with these findings/rulings, the LEDS code will need to adopt the following requirements at the very least the LEDS Code means the following requirements should be adopted in the very least. This will include commitments to;

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

NLEDP – Non-Paper

- a. Create and maintain in a single online publicly available place³ a Code of Practice for LEDS aimed at covering the principal scenarios in sufficient detail such that users, managers, suppliers, auditors etc will be able to determine what their duties are and understand whether they have been met,
- b. Create and maintain in a single online publicly available place a Guide aimed at increasing public understanding of the Code of Practice. Included in that public space the answers to frequently asked questions,
- c. Update the Code of Practice and public guide at least annually to take account of new developments or thinking,
- d. Consult on the wording of the Public guide to ensure it is comprehensive and easy to read,
- e. Update secondary sites of public knowledge and websites and keep them up to date and in line with the Code of Practice and public guide,
- f. Implement training, learning and development due to changes to the Code of Practice,
- g. Ensure that all relevant information is proactively placed into the public domain except where it needs to be redacted for operational or security reasons⁴. This will include the procedures and conditions that underpin the data and processing within LEDS,
- h. Ensure each organisation has a specific discipline policy in relation to misuse of data and to the extent possible it publishes the measures that it takes to protect against misuse of information and the numbers of disciplinary incidents,
- i. Ensure each organisation understands how to separate and keep separate sensitive (both operationally and data protection) information and that training is provided to all users on this point,
- j. Consult annually on the impact of the Code on privacy matters generally,
- k. Include information on public rights to access information held about them, including through the Freedom of Information Act and Data Subject Access Requests,
- l. Ensure automated deletion of information (including custody images) according to published schedules is taken in conjunction with local police records and, where practical, members of the public (or nominated representatives) are contacted and alerted to the deletion,
- m. Review and publish criteria for the rationale for retaining and deleting information, and,
- n. Implement within LEDS the Behavioural guidance and statistical monitoring to assist with identifying and protecting against arbitrary interference and

³ The assumption is this will be maintained by the College of Policing with input from law enforcement and policing, the Home Office and HMICFRS

⁴ These high-level decisions will need to be discussed to aid transparency.

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

abuse of power, e.g. including the guidance within Best Use of Stop/Search “BUSS” repeated stop and search.

Are there ways in which the commitments could be improved to take account of the court ruling?

10. Other key areas to address are below;

Organisational Standards

11. Organisational standards by which we mean the specification of principles and procedures by which each organisation ensures an appropriate operational environment.

- a. The Code will require support from Leadership within each organisation and therefore the Code will itemise the leadership behaviours⁵ expected from leaders at all levels,
- b. The Code will use and build upon emerging positions on the ethical use of data,
- c. The Code will include what the LEDS is not to be used for. Including non-work-related reasons,
- d. The Policy and Strategy in relation to the use of data within LEDS – what is the purpose of LEDS and why is it in place. What are the success criteria for LEDS and who will benefit from LEDS?
- e. The requirement for data sharing and partnership working and the resources this will require to ensure compliance,
- f. The key processes and people that will need to be in place within each organisation to ensure compliance with the Code and follow up from HMICFRS inspections,
- g. Internal and National Audit requirements. This links into evidential standards but also to ensure confidence that investigations and potentially disciplinary actions or prosecutions follow for breaches of the Code,
- h. The need for Training, Tradecraft and continuous professional development for all users to understand the requirements placed upon them by the Code and their duties to use the data for the purposes required.

⁵ Linked to the College of Policing Code of Ethics

Transparency

12. In the first instance, the Code will be statutory Parliamentary guidance. It will be necessary to monitor, with HMICFRS Her Majesty's Inspection of Constabulary Fire and Rescue Services (and other bodies as appropriate), to understand how effective this Code of Practice is.

13. Which bodies will have access to LEDS and why? This might be in a tabular format with each individual organisation and a summary view of the reasons why they access LEDS with statistics on how often. This should link to each organisation's relevant Data Protection Impact Assessment and to key points of the Protection of Freedoms Act.

14. A description of the law enforcement powers and activities that might be used in relation to accessing data on LEDS and the enabling legislation that underpins it. The Code of practice will include examples of information that will be shared, retained, accessed or processed during investigations, arrest, bail, detention, prosecution, court disposals and conviction. The Code will also include;
 - a. the legislation underpinning those activities,
 - b. definitions and sources of data, for example, information on driver and vehicle keeper information supplied by the DVLA and the restrictions on the use (processing) of that information,
 - c. Descriptions of how data kept as intelligence should be handled in a different way than data kept as a record of fact,
 - d. People whose data might be included on LEDS such as witnesses, victims and vulnerable persons, and how their information will be kept and processed separately.

15. LEDS reporting is expected to be managed through an annual inspection produced by HMICFRS and a response produced by the Home Office. The Home Office response will be combined with the publication of statistics on the use and operations on LEDS. The Home Office will work with independent groups to better ensure academic scrutiny of the statistics prior to publication.

NLEDP – Non-Paper

Jurisdictional differences

16. What principal differences exist for Scotland and Northern Ireland, Jersey, Guernsey, and Isle of Man in relation to any of the protections or procedures?
17. What arrangements, considerations or mechanisms should exist in advance of overseas data sharing or access to data overseas?

Should different considerations be implemented outside areas covered by European Convention on Human Rights as opposed to inside?

Data sharing agreements

18. LEDS user organisations will be covered under one single data sharing agreement. This same agreement will cover organisations that supply data to LEDS, but will link to individual Data Protection Impact Assessments produced.

Guidance

19. Relationship to other related guidance, for example on Authorised Professional Practice, and who (which body) maintains that other guidance.
20. Data obtained by Investigatory Powers, surveillance, communications data, covert intelligence. The Code should describe how that information should be marked and handled including if and how it should be shared with and what other specific caveats must be attached to the data⁶. The Code should include a brief description of the Investigatory Powers activity, point to the relevant Code and highlight any differences.

Data Quality

21. The measures that should be taken by each organisation using and supplying data to maximise data quality and minimise the possibility of poor data affecting an operational decision and therefore either unnecessarily interfering with privacy or liberty. This section of the Code will also set out requirements for systems connecting to LEDS and should provide the user of the Code with an understanding of the importance of data quality. The Code will also address ways of working and provide standards for Timeliness, Completeness,

⁶ Marking will be key to enable consistent responses in different organisations. Training and standards will be critical.

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

NLEDP – Non-Paper

Conformity, Duplication, Integrity and Accuracy. A dashboard is being created to enable organisations to routinely assess themselves against the standard.

22. Additionally, the Code will cover, training and accreditation, evidence (including disclosure), security, LEDES user access and separation through role based access controls, the inspection regimes and Audit.

Are all of the relevant additional areas covered here? How can the content of each of the areas be strengthened?

23. The topics described above have been drawn together into 4 aims within the proposed purpose statement below.

Proposed Purpose Statement for LEDES Code

Promoting Understanding - To ensure greater understanding of the objectives of LEDES as a law enforcement information system. This includes the users of LEDES such that they can be confident in the activities they need to undertake to prevent and detect crime and safeguard the public. This also includes the public so that they can be confident of the protections in place to safeguard their data and privacy interests.

Improving Performance - To construct and maintain a regime that delivers continuous improvements to the utility of the information within LEDES, including the data quality, the relevance of the information and the partnership working that requires information to be shared across organisational boundaries. The regime will also look rigorously and consistently at the information within LEDES and seek actively to delete information that does not have a proportionate law enforcement purpose and to end sharing of data sets where this is in the public interest. To the end of improving performance and greater automation of activities is promoted.

Driving Standards - providing practical support for the delivery of the Sustainable Development Goals (SDG) and the Government's plan for implementing those goals. Currently the most closely aligned goals including supporting how police, social services and others work together to protect vulnerable children (SDG 5 & 16), supporting the identification of victims of modern slavery (SDG 8), and the identification of the criminal networks involved in modern slavery and immigration crime (contributes to SDG 5, 8 & 16), and with the Ministry of Justice, supporting David Lammy's report on disproportionality in the criminal justice system (contributes to SDGs 5 and 10).

Promoting Fairness - to create the mechanisms (training, learning, development, audit and inspection) that will ensure that LEDES is not used in a way which is

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

NLEDP – Non-Paper

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.

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.

Appendix A. PNC Code purpose from page 7

- a) To set out achievable timeliness and quality criteria in relation to data entered onto the PNC.
- b) To promote the national adoption of good business practices to ensure the integrity of PNC data in the future.
- c) The PNC is the only full-time, operational national police computer system routinely supported by data from all police forces. It is the prime source of information in relation to the nominal record of offenders processed by the police, the courts and NPPAs (non-Police Prosecuting Authorities). As few of these agencies have update privilege, all inputting is undertaken by the police. Prompt updating of process originating outside the police service is dependent upon NPPAs expeditiously alerting the police to the commencement and conclusion of proceedings.
- d) Traditionally, a number of selected organisations have been authorised by PITO (Police Information and Technology Organisation) to view PNC records to support internal business processes, primarily relating to character assessment. In recent times, access to the PNC has been extended more widely via the Criminal Records Bureau, the effective functioning of which is dependent upon the accuracy and timeliness of PNC data.
- e) The efficiency of the criminal justice system and the effectiveness of the police are dependent upon the accuracy and timeliness of PNC records.

Appendix B.

The purpose of the existing PND Code.

- a) to promote the lawful and consistent use of the PND and the information obtained from it;
- b) to ensure that chief officers adopt practices for the use of the PND and the information obtained from it in order that such information is used effectively for policing purposes;
- c) to ensure that the operation of the PND complies with data protection and human rights legislation; and
- d) to ensure that the PND is not used in a way which 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;

This discussion document has been written to advance the formulation of Policy. It is not intended to be a statement of Home Office policy or intention.