

Code of Practice for the Law Enforcement Data Service: Questions to internal and external stakeholders

The Code of Practice on the use of the Law Enforcement Data Service (known as 'the Code' in this document) will govern the ethical sharing of data using the Law Enforcement Data Service (LEDS).

This consultation seeks views on the plan to provide for a Statutory Code under section 39A of the Police Act 1996 to facilitate the sharing and protection of LEDS data. It seeks views on the associated guidance documents and asks, for example, what further guidance should be provided to help organisations follow the rules, what training and support should be available. It also seeks views from those affected on the practical implications of complying with the requirements and the governance and oversight framework, and on the proposed procedure to ensure compliance with the obligations in the Code.

The Code has been written by the College of Policing in partnership with the Home Office. The National Law Enforcement Data Programme (NLEDP), a Home Office programme is building LEDS.

LEDS will replace the Police National Computer (PNC), which is primarily used by law enforcement, to record records of fact such as arrest, detention and conviction information. LEDS is planned to also replace the Police National Database (PND) which is the primary system used by the law enforcement community to share intelligence records. Historically those intelligence records are not used in evidence but to guide investigations. It is the intention of LEDS to bring together at the point of query information from both sources. LEDS will also include the National Register of Missing Persons (NRMP) to enable police to help locate those who are missing and safeguard those who may be vulnerable.

LEDS will start to provide the NRMP next year. The Police National Computer functionality will be added in 2021 and into 2022, with the final addition the Police National Database being added in early 2023.

The LEDS service will continue to develop following first launch and will have significant additional functionality released by 2023. Therefore, the Code may be updated as new functionality is added to LEDS. The first external consultation is due to start in October 2019, it will be in two parts starting with a formal consultation aimed at potential users and organisations providing oversight. The second part of the consultation is planned to start in April 2020 and it is hoped this will be accompanied by a broad public conversation about the LEDS capabilities. A second consultation is planned in 2021/2 to ensure any proposed changes when PND data is added to LEDS are accounted for. The Home Office commits to consulting periodically after this time when significant changes to the Code are required.

The Home Office has been working with Civil Society Organisations to better reflect a diverse range of views into the way LEDS will work. Those views are coordinated

by “Involve”¹. The Home Office is working with Involve who have established an Open Space for Civil Society and the Home Office to discuss matters related to LEDS. The responses to this Consultation will be assessed and analysed by the Home Office. To assist with transparency the Home Office will work with Involve to demonstrate how the consultation responses are reflected in any update to the Code. If you do not wish Involve to read any part of your response please indicate this.

How the new Code will replace the existing Codes?

The Code will initially replace the existing PNC Code dating from 2005 when that system is decommissioned. The PND Code written in 2010 will be withdrawn at the same time as the PND system is decommissioned. The new Code will introduce stronger measures aligned to greater human rights and data protections and will bring continuous professional development for all LEDS activities into scope as appropriate in each organisation. The Code aims to support more effective operational use and sharing of data and put in place the mechanisms that enable this. Additional material will be developed including training material based upon this Code.

The Code has been developed with some advice from certain Civil Society organisations who agreed to provide feedback due to their knowledge and expertise. Some of those organisations have given advice on the basis that the Home Office should not disclose their participation. Other Civil Society organisations are content for their participation to be known. The Home Office values that frank and constructive advice from Civil Society and intends to respect their choice of whether to disclose their involvement.

The Code builds on existing UK legislation such as within the Data Protection Act (2018) and the Human Rights Act (1998), which include public duties to use data to prevent and detect crime and to safeguard the public, but to do so in a proportionate, lawful, accountable, ethical and necessary way.

To aid the understanding of the Code and assist with the implementation and interpretation two guides have been produced. The first is a guide to the Code for operational practitioners whose organisations will be using LEDS. The second is for the public so they can better understand how their data might have got onto LEDS and how their data might be processed and how organisations use and share that data to better safeguard the public and prevent and detect crime.

The Code supports key principles in upholding fundamental human rights, demonstrating equal respect to all people, in accordance with the law. In particular, the seven 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 (DPA), underpin the Code. The Code will achieve this through five 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

¹ <https://www.involve.org.uk/our-work/our-projects/practice/how-can-civil-society-be-involved-shaping-law-enforcement-data>

accurate and joined-up information in order to bring offenders to justice, to prevent crime and better protect vulnerable people. Policing is not always about crime and LEDS will also include the National Missing Person's Register to enable police to help locate those who are missing and safeguard those who may be vulnerable.

- b. **Promoting accountability:** Ensuring activities undertaken in relation to LEDS have clear lines of responsibility so that each organisation (users and suppliers of data) understands and 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 system. 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, protect the public and safeguard the vulnerable. The public reader should be confident of the protections that the Code puts in place to preserve their data and privacy interests.
- d. **Enabling Performance:** Supporting law enforcement performance using shared data. There will be a quality management regime, which delivers continuous improvements to the value of the information within LEDS thereby the service to the public. This will include promoting better data quality, ensuring the relevance of the information and strengthening the partnership working where information is shared across organisations. This will be facilitated by training and a requirement for organisations to pro-actively support continuous improvement.
- e. **Promoting Fairness:** The public need confidence in the relevance of the information held. The Code supports 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 disability. The Code will be regularly reviewed so it is consistent with evolving Human Rights, Data Protection and Ethical Standards. The Code will adhere to relevant data protection legislation and other principles. This will be done to make sure that information retained by law enforcement is restricted to what can be considered proportionate, legal, accountable necessary and ethical.

Questions

1. **Having read the Code and the guidance material do you feel the 5 aims outlined have been implemented in the Code?**
 - a. **[Yes/No]**
 - b. **If not, please explain your reasoning. [Free text]**

2. Does the Code reflect a baseline for ethical practice in the use of a national data system for law enforcement?

- a. [Yes/No]
- b. If not, please explain your reasoning. [Free text]

How will the Code will take effect and when?

The Code will be consulted upon in two planned stages:

- LEDS Code consultation 1 - The first phase seeks a formal engagement with future LEDS organisations, those expected to be involved with the LEDS governance and those who have been involved in the planning for LEDS. On completion of this phase of the consultation the training material, processes and will be finalised. This will be followed by an explicit public consultation (planned for between April and October 2020) where the majority of the supporting information that can be published will be. In the first instance this will cover the NRMP in the greatest detail.
- LEDS Code consultation 2 – Subsequent consultations will take place when significant revisions to the Code are needed. For instance, when the PNC data is added to LEDS.
- The Code will be laid in Parliament prior to PNC or PND activities being conducted in LEDS.

Organisations that will be affected

The Code applies to all organisations that will use LEDS, these include;

- Police,
- Law enforcement organisations,
- Government departments and arms-length bodies,
- Third sector and
- Commercial organisations

A full list of organisations currently accessing PNC or PND is available at this location. [DN attach list] together with a summary of the data they have access to and why.

It is anticipated that they will sign data sharing agreements to access LEDS. The Code applies to all organisations that will supply data to LEDS and also to those bodies providing governance to and overseeing LEDS. It will also apply in part to organisations supplying systems to police forces and other organisations that connect to LEDS. The personal data within LEDS and who it applies to is described in the guide to the Code.

Questions

3. **Having read the Code and the guidance material do you understand the range of organisations involved in LEDS?**
 - c. [Yes/No]
 - d. If not, please explain your reasoning.

4. **Having read the Code and the guidance material do you understand what roles the organisations involved in LEDS will play?**
 - e. [Yes/No]
 - f. If not, please explain your reasoning? [Free text]

5. **Having read the Code and the guidance material do you understand how those organisations will process personal data? If not, please explain your reasoning.**
 - g. [Yes/No]
 - h. If not, please explain your reasoning? [Free text]

6. **Is the guidance sufficient?**
 - i. [Yes/No/Don't know]
 - j. If not, are there other sources of advice, guidance or specific legislation that should be cited? [Free text]

Exemptions - things the Code won't apply to

Courts and investigatory bodies

Some bodies, for example those providing oversight for some of the law enforcement organisations are not explicitly covered by the Code. This is to ensure that their investigative and supervisory role is not fettered. The Courts are similarly not obligated by the Code. Her Majesties Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) is the monitoring body for LEDS. It will monitor organisational compliance with the Code including the Home Office as owner of the LEDS platform. HMICFRS will also be invited to make suggestions for future improvements to the Code itself.

Conduct exempted from the Code

We accept that some future activities may not be specifically mentioned in the Code. We also accept that the Code should not fetter the discretion of the court in the administration of justice or the discretion which any organisation inspecting the use of LEDS may have. Nevertheless, the users of LEDS should be aware that we expect most activities which directly involve accessing LEDS or inputting to LEDS will be covered by the Code.

We also recognise that there will be cases in which data is taken from LEDS and used in local systems. This is particularly the case where fast operational decisions are needed especially those involving law enforcement of foreign jurisdictions. Data

transferred into other systems needs to be done in accordance with the DPA 2018 and needs to be recorded under the provisions of the Code, but its use will not be inspected in accordance with the Code. This is to maintain the ability for law enforcement to make operational decisions.

Questions

- 7. Do you understand the types of activity that will be exempt from the Code?**
 - a. [Yes/No/Don't know]
 - b. [Free Text]

- 8. Would your organisation's activities fall under this exemption?**
 - a. **Yes my organisation is exempt**
[Inspectorate/Court/Regulator/Other], **No my organisation will be bound by the Code** [LEDS User/Suppler], **Don't know/Not applicable** [DK/NA]
 - b. **To help us understand better, please tell us why your organisation's activities would be exempt or explain why you are not able to determine this (if applicable)** [Free text].

- 9. Do you agree with the exemption for Courts and Investigatory Bodies?**
Please explain your answer.
 - a. [Yes/No/Don't know]
 - b. **Any comment?** [Free text]

Disproportionate burden

The Code seeks to enhance operational performance through enhanced sharing of data, but it is recognised, in certain circumstances, meeting the requirements could increase the administrative overhead on a law enforcement body that is not proportionate to, for example, the size of the organisation, the number of users it has, or the cost of compliance.

Each LEDS user organisation must carry out the initial assessment of the extent to which the Code might impact them. If, on the basis of its assessment, a body decides the impact of meeting the Code would be disproportionate, it should explain this in its response to this consultation. It should include an explanation of what parts of the Code would be difficult to comply with, and any alternatives provided for.

Question

- 10. Having read the Code and associated material and thinking about your organisation, managers and users do you understand what new organisational measures are needed?**
 - a. [Yes/NO]
 - b. **Could the aims of the Code be met?**
 - c. **If not, please explain where any further explanations would be helpful.** [Free Text]

Questions

15. Does your organisation understand the need to implement the learning and training requirement that goes alongside the Code?

- a. [Yes/No/Don't know]
- b. If no, how can this be made clearer? [Free text answer]

16. What additional training/learning/guidance measures need to be implemented to make best use of LEDS? [Free text answer]

17. Is your organisation understand how to share data proportionately with other organisations and the measures needed to facilitate this?

- a. [Yes/No/Don't know]
- b. If yes any comment? If no, how can this be made clearer? [Free text answer]

Inspection

The Code endorses HMICFRS to monitor all user organisation's use of LEDS. This will include the Home Office as the provider of the LEDS platform.

Other Bodies will also have inspection governance and oversight roles, principally,

- Independent Office for Police Conduct (IOPC)
- Police Investigations and Review Commissioner (PIRC)
- Information Commissioner's Office (ICO)
- National Police Information Risk Management Team (NPRIMT)
- Biometrics Commissioner
- Surveillance Camera Commissioner
- Chief Inspector of Borders and Immigration
- Chief Inspector of Prisons
- Investigatory Powers Commissioner
- Investigatory Powers Tribunal

The Home Office is developing a governance and compliance structure for LEDS procedures which will assist law enforcement bodies with compliance and support them to ensure their activities are compliant. The expectation is that for material non-compliance with the Code that withdrawal of agreement to use LEDS is expected.

Question

18. Do you have any comments on proposed enforcement of the Code?

- a. [Yes/ No]
- b. Please elaborate [Free Text]

An impact assessment has been drafted defining the expected resources each organisation will require to comply with the Code. **[DN-to be drafted]**

Question

19. Are the governance arrangements for the Code clear and easy to understand?

- a. [Yes/ No]
- b. Any comments? [Free Text]

20. Thinking about the proposed layout and structure for the Code, do you feel it is clear and accessible?

- a. [Yes/ No]
- b. Any comments? [Free Text]

21. Is there any expected content missing from the Code or whether any existing content is superfluous, irrelevant, inaccurate or technically unsound?

- a. [Yes/ No]
- b. Any comments? [Free Text]

Additional material for the consultation website

A guide to the National Law Enforcement Data Programme and the Law Enforcement Data Service including further detail on the Police National Computer and Police National Database is available here.

What is the Management of Police Information

The College of Policing is responsible for the Authorised Professional Practice (APP) of the Management of Police Information. According to the College of Policing "...The principles of management of police information (MoPI) provide a way of balancing proportionality and necessity that are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information."

<https://www.app.college.police.uk/app-content/information-management/management-of-police-information/>

What is Part 3 of the Data Protection Act

The Law Enforcement Principles for Data Protection are set out in Part 3 of the Data Protection Act 2018 (DPA 2018). This implements an EU Directive (Directive 2016/680) dealing with how law enforcement should process personal data for law enforcement purposes. It is separate to but complements the General Data Protection Regime (GDPR). More information about it can be found on the Information Commissioner's Office website. There are no plans to change the UK's posture towards Data Protection.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/>

What are the Nolan principles?

The Seven principles of public life apply to anyone who works as a public office-holder. They are;

- Selflessness.
- Integrity.
- Objectivity.
- Accountability.
- Openness.
- Honesty.
- Leadership.

This includes people who are elected or appointed to public office, nationally and locally, and all people appointed to work in:

- the civil service
- local government
- the police
- the courts and probation services
- non-departmental public bodies
- health, education, social and care services

The principles also apply to all those in other sectors that deliver public services. Further information on the principles of public life and the committee that oversees them is available on the committee's website.

<https://www.gov.uk/government/organisations/the-committee-on-standards-in-public-life>

The Code of Ethics for Policing

In 2014 the College of Policing launched the Code of Ethics for Policing. The aim of this Code is to support each member of the policing profession to deliver the highest professional standards in their service to the public. It is available on the College's website.

https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf

The Code of Practice for the PNC [DN:provide a copy on the consultation site]

The existing Code of Practice for the operation and use of the Police National Computer was archived, but, is available here.

https://webarchive.nationalarchives.gov.uk/20060715171137/http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/Police_nat_comp.pdf?view=Standard&pubID=188851

The Code of Practice for the PND [DN:provide a copy on the consultation site]

The existing Code of Practice for the operation and use of the Police National Database is available here.

<https://www.gov.uk/government/publications/code-of-practice-on-the-operation-and-use-of-the-police-national-database>

Privacy Impact Assessment

A Privacy Impact Assessment for the planned Law Enforcement Data Service was published in 2018. Within the document is an updated privacy assessment of the Police National Database and the first ever privacy assessment of the Police National Computer. The next privacy assessment will be contained within a Data Protection Impact Assessment (DPIA). This document is being drafted and will be published by April 2020. A summary of the published PIA is included together with a summary of the intended changes for DPIA. **[DN. Summary document for the DPIA changes]**

<https://www.gov.uk/government/publications/law-enforcement-data-service-privacy-impact-assessment>

Current use of PNC and PND [DN:To be compiled]

A list of law enforcement organisations using PNC and PND is attached together with notes on what they use the systems for.