National Law Enforcement Data Programme:

LEDS: Code of Practice

Update Document

20 February 2019

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.

Introduction

1. This paper has been written to provide an update on the drafting of a Code of Practice (Code) for the combined Law Enforcement Data Service (LEDS). This paper itemises the recommendations gathered for the Code purpose statement and commitments during workshop 2 on 4th October 2018 (Action #12) and reflects those recommendations in an updated proposed structure.

2. Section 1 of the paper presents the background to the Code. Section 2 outlines a summary of the comments received at the October workshop and the Home Office response. Section 3 details the proposed Code structure updated to reflect the comments in section 2. If the Open Space members are content, this proposed structure will be used for drafting the Code.

3. Over the next three months the College of Policing will consult with law enforcement practitioners and relevant bodies to produce a first draft of the Code. This will be presented in May 2019 to the Open Space to critique and further refine. A consultation with practitioners is scheduled for September 2019 as a prelude to a full public consultation between June and September 2020.

Section 1 - Background

4. LEDS will replace the Police National Computer (PNC) in 2021 and the Police National Database (PND) in 2022 and therefore the existing PNC and PND Codes of Practice will need to be updated and merged. In addition to replacing the PNC and PND in 2020, a new National Register of Missing Persons (NRMP) will be established as a forerunner to LEDS in 2020.

5. The NRMP project will introduce a critical change to the way that information about missing people is managed. Currently information about missing vulnerable people is retained on the PNC for only such time as the person is missing. The information is deleted if the missing person is found. In many cases a person will be reported missing on more than one occasion and therefore critical information that could assist the police in locating the missing person will be deleted. The NRMP project is currently being defined. If there is specific interest from Open Space members a paper on NRMP will be presented at future meetings.

6. 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. This will require Chief Constables in England and Wales and their police forces to take account of the Code.

7. The Code will not, by itself, compel the police forces of the devolved administrations (Scotland or Northern Ireland, Channel Islands or Isle of Man) nor the non-police law enforcement bodies. However, all organisations that use LEDS will have to sign up to being bound by the Code including the inspection regime that underpins it.

Section 2 – Open Space comments and Home Office response

8. The Code of Practice paper in October 2018 suggested 4 aims; Promoting Understanding, Improving Performance, Driving Standards and Promoting Fairness[1]. Members suggested there should be a specific aim of "Safeguarding Citizens" to draw together the operational aims for LEDS into one paragraph. This additional aim will bring together the importance of using data for investigating crime and safeguarding citizens.

9. Members of the Open Space agreed improving performance of those using the data was critical for the Code and suggested the Code should also cover data entry, the data types that are on LEDS and a specific commitment around ensuring that data inputting is accurate. The Home Office agrees.

[1] Appendix A

10. Members wanted the statement on “Promoting Understanding” to be more explicit. The Home Office agrees.

11. Members of the Open Space wanted the term “fairness” to be expanded as they felt it to be too narrow. The section on “promoting fairness” will be redrafted to bring out the requirement to have protections for political and journalistic sources, as well as faith, legal and health practitioners. It will also make clear the requirement to protect data in alignment with data minimisation principles.

12. Members also wanted to ensure that the inclusion of data governance was made broader to include a human rights perspective, too. This is agreed.

13. Additionally, Members wanted a clearer articulation of accountability within the Code. It is proposed one of the aims of the Code should focus on accountability. Therefore “Promoting accountability” will sit as a new aim alongside “Safeguarding citizens”. Accountability will include both data governance and a separate statement on Human Rights. Driving standards and Improving Performance aims will be merged.

Additional requirements sought

14. Members of the Open Space wanted to ensure the Code will include a Governance outline including who to go to with whistleblowing concerns. The existence of the local whistleblowing arrangements will be part of the LEDS inspection regime. There will be references to national arrangements for whistleblowing contained in the Code (Action #15).

15. Members wanted the principle of data minimisation and ensuring the right data is retained within LEDS in the Code. This is agreed.

16. Members asked for a specific commitment regarding training. They wanted a national standard for training and an assurance that there will be structured training for LEDS and for this to be documented in the Code. The Home Office confirmed that manuals, multi-layered training and e-learning modules etc would be provided which would then be linked to access controls. The Home Office has appointed a learning partner. The Code needs to link with police training and those supporting service delivery.

Consultation and review

17. The Home Office committed to holding a formal Public Consultation on the Code of Practice. This paper confirms a commitment to doing this prior to laying the Code in Parliament (Action #13). Following the input provided by Open Space members the Home Office intends to refine the Code with the user community in a transparent way. The draft Code will be placed in the

public domain as will the updated version following formal consultation with practitioners. This updated version will have a formal three-month Public Consultation. The Home Office desires an informed public debate to precede that public consultation and will discuss ideas for making that happen. Nearer the time, we would welcome input from the Open Space into the proposed format of consultation questions.

18. The Home Office will make available a limited number of hard copies of the LEDS Code after publication, this will be in addition to the online materials that will have accessible versions (Action #14). There will be Welsh language versions of the Code including for consultation.

19. Updates to the Code. It is recognised that the Code will need to be reviewed annually and refreshed as required. This will be driven through the inspection regime (HMICFRS) and environmental changes including legislative and case law changes. It will also be driven by regulators; such as the Information Commissioner's Office and oversight bodies; such as the Independent Office for Police Conduct (England and Wales), Police Investigations and Review Commissioner (Scotland) and Police Ombudsman for Northern Ireland. It is anticipated that the Public Guide will need to be refreshed more frequently. The Home Office will maintain through the College of Policing a capability to proactively canvas suggestions to refresh the Code throughout the year.

20. Members wanted a commitment to consult annually on the Code on privacy matters generally, but also to maintain interim updates where there is an indication that either the Code or the Guide need refreshing. The role of HMICFRS (Her Majesty's Inspection of Constabulary Fire and Rescue Services) is to be defined and agreed between HMICFRS, the Home Office and Policing with input from Open Space members.

21. It is also the case that outside of the formal inspection and review processes relevant experiences will be identified. In addition to ideas from user organisations ideas for improvements might be generated by interested bodies. To ensure these ideas are captured and assessed the Home Office, through the College of Policing, will maintain an ability to receive suggestions and have these assessed for inclusion in either the Code or the public guide. This mechanism will be used to inform an annual review of the Code (Action #11).

Protections

22. Members of the Open Space wanted a clearer statement that journalist sources, medical professionals, legal professional privilege and matters of conscience will be protected. The Home Office agrees.

Transparency

23. Members of the Open Space asked whether there could be different Codes for data on victims and suspects / people with convictions, however, the Home Office suggested that this should not be necessary and will ensure the Code has a section on strict access controls. This could be revisited when the Code is drafted if the separation is not sufficiently clear.

24. Members also asked whether there could be access controls for investigators and wanted a clear statement and policy to prevent investigators from searching personal information or any information on family members etc. The Home Office agreed to this statement.

25. The Code needs to reflect wider usage in other law enforcement bodies. The Home Office clarified that LEDS is not planning to seek legislative change to add additional organisations.

26. Members of the Open Space wanted to ensure that a section on data sharing was included in the Code. This will be included.

27. Members of the Open Space were keen to include an explicit statement covering the supply of LEDS data law enforcement organisations in countries where the Capital Punishment is still permitted. This will be considered; we will consult with Law Enforcement Colleagues over the next three months.

28. Members of the Open Space were concerned about Data Subject Access Requests (DSAR). The Code must be clear about how to challenge data held about individuals and how this could be rectified or deleted data. This should include information about the fact that not all LEDS users will be able to see all information as Access controls could stop users responding to subject access requests. This point needs to be clarified by the Home Office. The Public will expect a single access point for the DSAR and it needs to be clear what information is available for deletion/modification/challenge.

29. Members of the Open Space wanted transparency to be maintained over who will be maintaining the system, i.e. contractors outside government. The Home Office clarified that the intention for this to be a Home Office service and for contractors to be embedded within Home Office. Where this affects the Code or Governance regimes the Code will call for this transparency to be maintained.

30. Members of the Open Space asked what safeguards were in place to ensure quality and purpose of data. Members also asked what measures were in place to ensure that deletion was a possibility, including automated deletion, where practicable. The Home Office confirmed that LEDS would include a comprehensive deletion capability functionality and was designing governance to reflect this.

31. Members of the Open Space wanted reassurance about any impact the Good Friday Agreement might have on the multiple jurisdictional nature of LEDS. Members wanted to know what protections would be in the Code. The Home Office is committed to consulting with the appropriate public bodies, police and Civil Society Organisations concerning this area.

32. The Home Office would like to see an independent academic/civil society public report compiled annually on the operation of LEDS. This would summarise Open Space discussions, progress and suggest further areas for improvement.

Section C - Updated Proposed Code Structure

1. The LEDS Code will need to adopt the following requirements at the very least. This will include commitments to;

   a. create and maintain in a single online publicly available place[2] 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 a single online publicly available guide[3] 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 reasons[3]. 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 under data protection laws) information and that training is provided to all users on this point,

[2] The assumption is this will be maintained by the Home Office on Gov.UK (Internet facing) by the Home Office with a link to the College of Policing website and a summary on "Polka" (the Police OnLine Knowledge Area) with input from law enforcement and policing, the Home Office and HMICFRS

[3] These high-level decisions will need to be discussed to aid transparency.

j. Consult annually on the impact of the Code on privacy matters generally, but to also to maintain interim updates where there is an indication the Code of Practice and the Guide need refreshing,

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,

n. Implement within LEDS the behavioural guidance and statistical monitoring to assist with identifying and protecting against arbitrary interference and abuse of power, e.g. including the guidance within Best Use of Stop/Search “BUSS” repeated stop and search,

o. The College of Policing to ensure that all materials are appropriately “accessible” and written in plain language. There will be Welsh language versions of the Code including for consultation,

p. HMICFRS to tell the Home Office where the Code needs updating. This responsibility is to be specified in the Code,

q. The resources needed by HMICFRS to be subject of a discussion by HMICFRS and the Home Office when the annual plan is set,

r. Need to proactively reach out to other regulators that might have an interest in LEDS and build a “RACI” (Responsible, Accountable, Consulted Informed) matrix,

s. Each LEDS organisation should nominate a senior person to be the point of contact for compliance with inspections under the Code, and,

t. The Business Service team in LEDS will assess each organisation’s administrative documents during the onboarding process and signing of the Data Sharing Agreement.

2. Other key areas to address are below;

Organisational Standards

3. 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 behaviours[4] 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,

    i. The Code will use the Nolan principles for standards in public life and the Code of Ethics for Policing.

    Transparency

4. In the first instance, the Code will be statutory Parliamentary guidance. It will be necessary to monitor, with HMICFRS (and other bodies as appropriate

[4] Linked to the College of Policing Code of Ethics

such as the Information Commissioner's Office and Biometrics Commissioner), to understand how effective this Code of Practice is.

5. Which bodies will have access to LEDS and why? Police are the majority user of LEDS, but the Code needs to reflect wider usage in other law enforcement bodies. A definition of law enforcement will be provided with a list of bodies that have access to LEDS/PNC/PND. This will 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. In relation to LEDS this should link to each organisation's relevant Data Protection Impact Assessment and to key points of the Protection of Freedoms Act.

6. 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 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.

7. There will be a formal three-month Public Consultation. The Code will be reviewed annually in future.

8. 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.

<u>Jurisdictional differences</u>

9. What principal differences exist for Scotland and Northern Ireland, Jersey, Guernsey, and Isle of Man in relation to any of the protections or procedures?

10. What arrangements, considerations or mechanisms should exist in advance of overseas data sharing or access to data overseas?

Data sharing agreements

11. 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.

12. An explicit statement should cover the use of LEDS data and interaction with law enforcement organisations in countries where the Capital Punishment is still permitted.

Guidance

13. Relationship to other related guidance, for example on Authorised Professional Practice, and who (which body) maintains that other guidance.

14. 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 data[5]. The Code should include a brief description of the Investigatory Powers activity, point to the relevant Code and highlight any differences.

Data Quality

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

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

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

Proposed Purpose Statement for LEDS Code

The purpose of the Code is to support the ethical, fair, diligent and impartial use of the LEDS system and through so doing upholding fundamental human rights and equal respect to all people, according to law, the principles of holding a public office and the Code of Ethics for Policing.

The Code will achieve this through 5 equally important aims:-

Safeguarding citizens: - Facilitate the use of data by law enforcement and other agencies at the appropriate time and in the appropriate way of accurate and joined-up information in order to prevent crime and better protect the public. A Code that increases the ability to bring offenders to justice.

This Code of Practice will facilitate digital collaboration between different law enforcement organisations and the criminal justice sector in a more efficient and effective way. It will better ensure alignment to MOPI (Management of Police Information) and other principles, thereby minimising the amount of information retained by law enforcement.

Promoting accountability – To ensure activities undertaken in relation to LEDS have clear lines of accountability. All LEDS user organisations will be required to sign up to a Data Sharing Agreement which will make adherence to the Code mandatory.

Before access to LEDS is granted each organisation will have to demonstrate how their organisation meets the standards within the Code. This will include an assessment of organisational standards and a commitment to the inspection regime.

DSA will require organisations and users to be compliant with the Code and its requirements on data governance.

Each organisation (user and supplier) needs to ensure they can demonstrate that they meet the principles in the Code. The Code will use the Nolan principles for standards in public life and the Code of Ethics for Policing

This will mean;

- All involved with LEDS (Users, Supervisors, Managers, Leaders, Suppliers) being appropriately trained for the role that is being undertaken.
- All LEDS user organisations itemising their powers to use LEDS information and having those publicly accessible

In order to ensure compliance with the standards outlined in the Code the Business Service team in LEDS will assess each organisation's administrative documents during the onboarding process and signing of the Data Sharing Agreement. Each LEDS organisation (user and data suppliers) should nominate a senior person to be

the point of contact for compliance with inspections under the Code. LEDS organisations should consider the impact of Human Rights particularly on people with protected characteristics. This should be reflected in the organisation's Data Protection Impact Assessment.

Promoting Understanding - To ensure greater understanding of the objectives of LEDS as a law enforcement information system. This includes the users of LEDS 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.

User organisations will be required to ensure appropriate training, learning and development for the use of LEDS. The College of Policing and the Home Office will develop the framework through which this can occur.

Enabling Performance: - To construct and maintain a regime that delivers continuous improvements to the utility of the information within LEDS, 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 LEDS 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.

The Code will also cover the Home Office duties in relation to LEDS. It is acknowledged that these duties will need to be open to inspection.

Promoting Fairness - to create the mechanisms (training, learning, development, audit and inspection) that will ensure that LEDS 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. Ensuring the Code is reviewed against and maintained consistent with evolving Human Rights, Data Protection and Ethical Standards. This will include if and how journalists, faith and conscience practitioners, legal and health practitioners are affected by LEDS.

List of Processes – The Code is proposed to have sections on the following;

- Obtaining data
- Inputting data
- Sharing data
- Protecting data
- Accessing data
- Using data
- Removing data

The Code will have Statements on at least the following;

- Governance
- Whistleblowing Concerns
- Training
- Service Delivery
- Review and Consultation of the Code and,
- Unacceptable uses of LEDS system or information.

Appendix A

Promoting Understanding - To ensure greater understanding of the objectives of LEDS as a law enforcement information system. This includes the users of LEDS 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 LEDS, 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 LEDS 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 LEDS 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. Ensuring the Code is reviewed against and maintained consistent with evolving Human Rights, Data Protection and Ethical Standards.