LEDS Open Space Non-Paper

LEDS Open Space:

LEDS: Code of Practice

Update Document

This Document has been written with the aim of stimulating discussion on the development of 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 and viewed only by members of the LEDS Open Space.

Significant changes to document

30th April 2019

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

Purpose

This paper has been written to provide an update on the drafting of a Code of Practice (Code) for the Law Enforcement Data Service (LEDS). This paper will be discussed within the LEDS Open Space on 14th May 2019 and will aim to provide an update on the project progress since the last Open Space Meeting in February, to promote further discussion on proposed content and structure of the Code and identify how the considerations of previous workshops have been taken into account in early drafting. This paper discusses the Code specifically rather than wider issues around the NLEDP and the development of LEDS.

Summary

This paper provides an overview of the status of the Code. In reviewing this and attached documents members of the Open Space will be asked for their views on the current drafting structure, indicative content and proposed formatting.

Key questions posed by this paper

1. Whether the current drafting structure covers what was anticipated following earlier workshops and provides confidence in the drafting process?
2. If not, what are the gaps that are emerging?
3. Is it clear enough as to who is the intended audience for the Code?
4. Is it clear as to how the Code will be used by?
    - 4.1. The Home Office?
    - 4.2. Organisations accessing LEDS?
    - 4.3. Managers of those using LEDS in their day to day working practice?
    - 4.4. Individuals using LEDS in their day to day working practice?
    - 4.5. The public and stakeholders who are interested in ethical law enforcement practice?
    - 4.6. Those whose data may be held on LEDS?

Update Document

Progress on Drafting

1. Two College of Policing contractors started work at the end of 2018. Consultation workshops with both Police and non-Police were held in April 2019. Staff changes have caused some delay – one contractor left and has since been replaced.

2. The Home Office and the College of Policing have a Project Steering Group to provide direction to drafting the Code of Practice. The indicative timeline agreed with the Steering Group at the end of December 2018 was:

    - Iteration 1 (70% of topics) - end of May 2019
    - Public Guide to Code - end of July 2019
    - Iteration 2 (95% of topics) - end of September 2019
    - Final draft Code of Practice - Jan 2020
    - 6 months consultation - July 2020
    - Final proof - August 2020
    - Further public consultation (3 months) - November 2020
    - Publish the Code - Dec 2020

    Following these changes we anticipate the draft Code document being available in June 2019. This will not affect remaining milestones as the proposed circulation of the draft Code for user consultation will continue whilst drafting of the Public Guide is underway.

3. The drafting team have met subject specialists and will continue to do so throughout May to better understand the detail required in ascribing best practice to the data functions and supporting functions which will form the main Code material.

4. The consultation with current PNC and PND users focussed on the proposed structure and intentions of the Code and to enable direct users (data inputters, data analysts, professional standards specialists and such like) to provide input into the what 'best practice' might look like against the headings of the Code. This information is currently being processed. The most recent version of the draft structure is included below. Attached as an annex paper is a very draft example of what a section might look like.

5. The drafting is intended to be user-friendly and accessible so that the document is more actively referenced. We expect a more formal opening section, Part A, to be detachable and will be in the format needed for laying before Parliament. We will refer to existing guidance documents which have been developed by the College of Policing, the Code of Ethics for Policing. The Code of Ethics will be referenced within the Code of Practice for

LEDS. The Code of Ethics for Policing will be circulated to Open Space members with this paper.

Specific points raised by Open Space Members at earlier meetings

6. With reference to the previous papers submitted and discussed at previous Open Space meetings, the following points have been incorporated into drafting and development of the Code:

6.1. The statement of purpose now includes five aims, with Safeguarding People and Promoting Accountability in inclusion. The aims will be linked to the 'why' elements within the main text.

6.2. Avenues of recourse for individuals who identify any breach of the Code will be identified within the preamble. This will include provisions for those who may be deemed whistleblowers.

6.3. Issues concerning data inclusion and retention will cover fairness and proportionality and will reference updated guidance for policing Authorised Professional Practice for Retention, Review and Disposal. The Provisions of the Data Protection Act 2018 are also underlined and clarified in respect of the processing of personal data for law enforcement purposes. Specific guidance is being sought from a specialist in this field.

6.4. The application of documents such as Authorised Professional Practice, which are developed solely to guide Policing will need to be explored further in the light of the wider audience of organisational users who may not have access to such detailed and comprehensive guidance.

6.5. Training is included as a support function. The Home Office have undertaken to ensure that a full training programme will be developed for LEDS for all users, and the Code will also contain provisions for continuous professional development.

6.6. The review mechanism for the Code, once clarified will be agreed within the statutory element.

6.7. There is no intention to develop a separate Code for data on victims and suspects. Data in relation to victims and witnesses will be treated differently within LEDS and will be appropriately marked and viewed in more restricted circumstances. The Code will reiterate the principles of lawful purpose and reasonableness of processing data in the relevant sections. This will particularly be so in relation to victims and witnesses where the issue of "consent" following an incident will need to be more carefully considered.

6.8. The first iteration of the Code is to be available for the LEDS pilot of the National Register of Missing Persons.

6.9. Access controls will be included under the relevant data functions and there will be specific reference to inappropriate access and the consequences of misuse for both organisations and individuals.

6.10. Data sharing is covered as a specific section and this will include reference to the sharing of data across borders, and the European Court of Human Rights guidance on adequate levels of protection and assurances given that the data will not be used for any form of cruel and inhuman treatment, including the death penalty.

6.11. The provisions for Data Subject Access Requests are still to be clarified. Currently these are provided by ACRO, and there is no question about the continuance, but, there is a live debate about making disclosures more consistent.

6.12. As the Code will be housed electronically a list of who is accessing LEDS can be linked to the access point, the Code itself will show that it is open to wider law enforcement agencies but as it is likely to be required to be printable and version controlled such a list needs to be kept as a separate document.

Discussion document - Draft Structure for Code of Practice for LEDS

7. 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.

Overall Structure of the Code of Practice document

8. The Code of Practice document is a formal legal document which will be laid before Parliament it therefore will require some legal and formal text to cover this provenance.

9. It is therefore anticipated that the Code will be written in two parts, plus appendices. Part One will be the 'official' element and will be detachable so that the user version, in Part Two, can be easier to read. Police forces will be the main users (by volume) of LEDS, but, as with PNC and, to a lesser extent PND, other law enforcement and partner organisations will also have access, and the Code is therefore written to the wider audience of user. In addition, some private and public-sector organisations will also have access; to provide data used by law enforcement and in their commercial operations where there is a legitimate need; say, to prevent or detect fraud. They will be subject to the provisions of Data Sharing Agreements, which will require compliance with the Code of Practice.

10. In addition, there will be a publicly available Guide to the Code which will explain the background to LEDS.

Audience:

11. The Code of Practice should address all relevant audience sections, including;

    a. Strategic Law Enforcement leaders with accountability for data usage at organisational level who need to ensure appropriate systems needed for effective and efficient LEDS operations are established in each organisation.
    b. Operational Law Enforcement managers with oversight of processes and people in all Law Enforcement Bodies that will use LEDS.
    c. Operational End Users who will interact with LEDS in an operational capacity. Understand their responsibilities and give legal effect to those duties. In particular;
        i. duties around record keeping, data retention (weeding), data and device security, data sharing, data quality,
        ii. duties around ethical behaviours in relation to LEDS investigations,
        iii. national oversight, audit and record keeping,
        iv. importance of maintaining currency with LEDS training and development, particularly ongoing tradecraft updates,
    d. Law Enforcement Risk Owners who are responsible for data systems owning the compliance responsibility.
    e. Audit and Oversight bodies, especially Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS), Independent Office for Police Conduct, Information Commissioner's Office and Professional standards bodies.
    f. Public and Third Sector Partner agencies who need to understand how their data will be used if it is provided
    g. Private sector agencies who provide data and will want to know how their data is used. They also consume data and will need to implement new processes.
    h. Members of the Public, and those that might represent their interests under human rights protection which will need to be satisfied. This includes a (qualified) right to certainty (foreseeability) over what and how their data is (or as importantly could be) used within LEDS, and also how to get access to, change or delete their information.

<u>Proposed Purpose Statement for LEDS Code</u>

12. 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:-

13. <u>Safeguarding people: -</u> 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[i]. 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.

14. 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[ii]. 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[iii]

15. 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.[iv]

16. 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.[v]

17. 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[vi].

Discussion document - Draft Skeleton outline of the Code of Practice for LEDS

Part One:

Legal Background

- Statutory remit (including geographical jurisdiction)
- Enabling legislation
- Relationship to other guidance
- Concerned Bodies
- Review mechanism
- Dates

Introduction to the Code

There would be preamble with:

- Introduction to LEDS – governance and need for Code/ training
- Statement of Purpose (overarching principles)
- Definitions of Law Enforcement – related agencies and operations
- Intended audience

Responsibilities and Compliance

- Responsibilities for governance of LEDS
- Responsibilities and obligations to comply with the Code for leaders, managers and users of LEDS within organisations
- Role of HMICFRS

Ownership of data and accompanying responsibilities

- Data Protection Act definitions and relationships
- Organisational responsibilities under DPA/GDPR

Recourse

Remedies available to anyone who believes that data functions of LEDS have been inappropriately used, including those who might be considered as requiring protection for 'Whistleblowing'

Contributing bodies

Part Two

The Code of Practice

Introduction

The 5 Aims

Definitions of Data Functions

Structure of the document

- Data functions and attached supporting responsibilities
- Appendices
- Glossary

Sections

These are divided between Data Processing Functions and Supporting Functions, with sub-headings

Under each sub-heading there will be a header box with explanatory text, (currently the suggestion is to be grouped under Why, What and Further Guidance but with drafting the organisation of text may change)

What do we need to do to meet this requirement?

Then up to four sub-sections with the specific responsibilities to meet the Code:

The Home Office is responsible for:

A Law Enforcement organisation who has been granted access to LEDS will be responsible for:

As an operational manager within the organisation you will be responsible for;

As a LEDS user you are responsible for …..

Data Processing Functions

Inputting and amending data records:

- National record creation and associated processes:
- Validating Data
- Amending Data
- Updating Data
- Merging Data
- Storing Data
- Retaining Data
- Deleting Data

Accessing Data:

- Searching and Viewing Data
- Sharing Data
- Transmitting Data
- Exporting Data
- Disclosing Data

Using Data:

- Analysing Data
- Reviewing Data
- Applying Data
- Reporting Data

Supporting Functions:

Security of Data

Auditing of Data access and usage

Quality Assurance

Compliance

Training and competence

- Training for new users of the system
- CPD expectations

Malpractice

How organisations should treat evidence of malpractice

Notes:

[i] For the purposes of the Code this aim of Safeguarding will also extend to protecting property and animals, either wild or domesticated.

[ii] 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.

[iii] 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.

[iv] 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.

[v] 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.

At the time of writing the exact structure for governance of LEDS is still under discussion. For the purposes of drafting, a level of responsibilities has been ascribed to the Home Office which will be substituted by whichever organisation/body becomes the LEDS sustainment organisation.

[vi] This will include if and how journalists, faith and conscience practitioners, legal and health practitioners are affected by LEDS.