College of Policing

college.police.uk

Code of Practice for the Law Enforcement Data Service (LEDS)

Consultation questions

We welcome responses to the questions set out in this consultation paper.

Public consultation on the Code of Practice for the Law Enforcement Data Service (LEDS)

Stakeholders and members of the public are invited to answer the following questions, having read the Code of Practice, guidance document and other guidance material provided.

The last 10 questions relate to Police National Computer (PNC), Police National Database (PND) and LEDS user organisations. Members of the public should only complete the first 10 questions and the registration details.

This consultation is being conducted in partnership with the Home Office and your responses will be shared with them. If you consider any part of your response to be confidential, please indicate this here, stating which questions this confidentiality extends to and why.

Consultation questions

Your organisation

Are you answering as:

☐	An interested individual acting in a private capacity (for example, providing your views as a member of the public) Members of the public who are not part of an organisation involved in LEDS should tick this box and answer the first 10 questions only.
☐	An individual acting in a professional capacity
✔	On behalf of an organisation
	Please specify the name of your organisation: Privacy International (PI)
☐	Other (for example, a devolved administration)
	If other, please specify: (Please summarise your organisation or the people who you represent in the details at the end of the questionnaire)

Content of the Code

Q1 Thinking about the proposed layout, structure and language used for the Code and guidance document, do you feel it is clear and understandable?

Strongly agree	Agree	Neither agree nor disagree	Disagree ✔	Strongly disagree

If you disagree, please let us know why

Brief reference to the Nolan Principles addresses neither the reality of policing in the 21st Century, nor the ongoing real-time use of massive databases in the modern age. Concrete information is needed in the final Code around the safeguards that will be implemented, how role-based access controls will be allocated and reviewed in the future, who will oversee this process, the data that will be kept, and the extent to which it will be shared with other organisations and third parties. The Scope of the Code (section 4) needs to be clarified as it states that it *should be considered by organisations* ***other than police forces in England and Wales.*** This causes significant confusion in its current form. Does it mean that the code is not applicable to police forces in England and Wales and only to "other agencies within the United Kingdom that can access LEDS and selected data sets"?

Q2 Do you feel that the Code and Guidance Document effectively support the implementation of the five aims that are outlined on page 6 of the Code (safeguarding people, promoting accountability, promoting understanding, enabling performance and promoting fairness)?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree ✔

If you disagree, please let us know why

The Code and Guidance Document are ambiguous, talk in the abstract, and fail to explain in any real detail how these five aims will be achieved, implemented, or measured. LEDS must be not only subject to strong oversight, safeguards, and transparency, but also these measures must be clear and implementable, with direct lines of responsibility. It remains unclear how those individuals entered on the LEDS database will be safeguarded against deliberate misuse of their data, or from incorrect or invalid data. We highly recommend the implementation of a robust system of redress to allow individuals to challenge their inclusion in LEDS if they fear it to be unlawful, as well as sufficient transparency to allow individuals to understand if they are included. PI recommends implementation of robust controls to ensure that the images and data contained in LEDS cannot be used for any other purposes. PI is aware that access to DVLA data through LEDS will occur via an API interface that will allow access to DVLA but **no copying would be allowed**. We strongly recommend adopting the same mechanism for all data contained in LEDS, to reduce risks of misuse and to preserve data quality

Q3 Do the Code and Guidance Document set out and explain the ethical principles that individuals and organisations using LEDS should follow?

Strongly agree	Agree	Neither agree nor disagree	Disagree ✔	Strongly disagree ✔

If you disagree, please let us know why

These principles are insufficient as safeguards for users and organisations to ensure their compliance with the ethical standards, human rights and equality principles. The inclusion of intelligence material within the scope of LEDS, and therefore its provision by default to the numerous users and organisations rapidly increases the risks of misuse or other exploitation of such data. We believe that there should be clearer rules that will provide greater foreseeability about when, why and how the police and other third parties are able to use and access LEDS. Robust policies and procedures must be put in place to ensure the appropriate handling and deletion of data. More transparency is needed surrounding the way role-based access controls will be assigned, controlled, monitored, and publicly notified. There should be further guidance on how police forces should engage with individuals whose data has been stored on LEDS to inform them and what their rights are. Details of the redress or disciplinary procedures as a result of misuse of LEDS should be made clear. LEDS users should publicly disclose what access they have, how individuals can exercise their data rights, and how to seek redress.

Q4 Do the Code and guidance document make clear the range of organisations involved in LEDS, the roles of those organisations and how those organisations should process personal data?
(A list of organisations with access to LEDS data is available on the college.police.uk consultation page.)

Strongly agree	Agree	Neither agree nor disagree	Disagree ✔	Strongly disagree ✔

If you disagree, please let us know why

We are aware that the current list of organisations with access to LEDS is not exhaustive. Other organisations could be added to the list at a future date, as deemed necessary. We also note that in the longer term, the Home Office seeks to enable further data sharing between a range of organisations through the addition and integration of more systems to the platform or through links to systems owned by other organisations. Given the serious risk of function creep, any addition of new data sources or access rights **must be subject to parliamentary and public scrutiny and transparency.** The Code and guidance document should be very clear on how additional organisations will be given access to LEDS and **should include a consultation process** for such addition where the organisation proposed serves a purpose different from core law enforcement, such as the Border Force or state benefit organisations. Similarly, there is no mention of either how or if contractors and companies involved in developing, maintaining, or providing staff for the use of LEDS will have access. Given that commercial organisations are involved in the development of LEDS and provide staff to the Home Office and other government bodies, they should be included in the Code.

Q5 Thinking about privacy laws and regulations, do the Code and Guidance Document clearly set out the performance expectations and behaviours for LEDS users?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree ✔

If you disagree, please let us know why

The consultation documents are restricted to principles and do not deal in detail with any problems that LEDS poses for privacy rights and data protection. The creation of LEDS leads to the spectre of access by default to incredibly powerful wide-ranging capabilities, far greater than the sum of their parts. We believe that LEDS will also facilitate rapid checks of people's immigration status. Police already use mobile fingerprint devices linked to IABS. There should be clear querying and escalation guidelines against LEDS, in line with minimum access controls. The police should not be regularly accessing information outside their immediate policing need. Appropriate safeguards must be in place to ensure that LEDS is not used for immigration enforcement. LEDS must not be compiled with AFR technology or used to create local police databases and 'watchlists'. A mandatory Data Protection Impact Assessment should be made public to increase transparency about the use of LEDS and replace the existing privacy impact assessment. This should be implemented across England and Wales, to increase public confidence in the accountability of the police and the criminal justice process when using this intrusive 'mega-database'.

Q6 Do the Code and Guidance Document clearly set out that all LEDS users should be given appropriate initial and refresher training?

Strongly agree	Agree	Neither agree nor disagree	Disagree ✔	Strongly disagree

If you disagree, please let us know why

We are concerned that any training without due regard risks being little more than a tick-box exercise. It is crucial that training is effective and deals with issues such as what data would be deemed accurate and reliable, when the data from LEDS should be deleted, when it should be accessed and to what extent it should be shared. It is also necessary that there are no discrepancies in the understanding of the relevant data protection legislation and human rights amongst local police forces and constabularies. Appropriate and effective training is crucial considering that LEDS will contain a **significant** amount of data previously reserved for intelligence rather than evidential purposes. This may include subjective information from first-hand experience of the reporting officer, from covert human intelligence sources, and from lawfully authorised technical deployments such as trackers or listening devices. The nature of intelligence material is such that it is very unlikely to ever be subject to scrutiny or challenge. Training should also address how and when intelligence material should be recorded, the limitations on its reliability, and when it should be shared with other organisations, if at all.

Q7 Does the Code state clearly that users have a responsibility to ensure that data held in LEDS is of the highest possible quality?

Strongly agree	Agree	Neither agree nor disagree	Disagree ✔	Strongly disagree ✔

If you disagree, please let us know why

The consultation documents talk in the abstract, failing to explain to the users *how* they can comply with their responsibility that data held in LEDS is of highest possible quality, what this means in practice, or how this will be measured. Considering the broad nature of sources of data, together with the fact that data will consist of intelligence material, it is very difficult, if not impossible, to ensure that data entered is of highest quality and accurate. Those inaccuracies may go un-corrected for a considerable period of time. The code fails to provide sufficient safeguards to ensure that the data is of highest possible quality. By developing the technical capability in the backend to converge disparate data and make it more easily accessible, it will allow more authorities to access more data. This means that whatever access controls are put in place at the moment, they are subject to change and at the discretion of decisions made by whoever is in power in the future. It is essential therefore to ensure the system and decision-making process is as transparent as possible and subject to sufficient oversight. Potential biases in the system must be routinely interrogated and eliminated.

Q8 Does the Code clearly set out that personal data collected for law enforcement purposes and stored in LEDS needs to be lawful, adequate, relevant and not excessive in relation to the purpose for which it is processed?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree ✔

If you disagree, please let us know why

The data on LEDS will be drawn from a broad range of sources and will include intelligence as well as evidential material. LEDS will not just provide access to information contained in the PND and the PNC, but also a number of different other data systems used by forces. As a result, it is difficult to understand how it will be ensured that the data stored in LEDS will be lawful, adequate, relevant, and not excessive. The very nature of LEDS appears to be to combine data in an excessive form, without necessarily understanding its relevance to a particular operation, especially when subjective intelligence material is included. It is also difficult to see how data processed and stored in LEDS will be lawful, adequate, relevant and not excessive considering the lack of clarity as to what images will exist on LEDS once the PND and PNC are combined. There are currently about 12 million images enrolled into the PND gallery, some of which are retained unlawfully. Considering that the Code and the Guidance document fails to address these issues, it cannot be said that it clearly sets out that the data in LEDS needs to be lawful, adequate, relevant and not excessive.

Q9 Are the governance arrangements for maintaining the Code clear and easy to understand?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree ✔

If you disagree, please let us know why

No, they are not. The Code and its Guidance Document clearly state the exact governance structure for LEDS is still under discussion, therefore the documents *by definition* lack sufficient detail for this to be clear and easy to understand.

Exemptions – when the Code and Guidance Document do not apply

Q10 Do the Code and Guidance Document clearly explain the types of activity that will be exempt from the Code?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree ✔

If you disagree, please let us know why

None of the consultation documents (the Code, the Guidance and the Public Guide) contain a section outlining what the exemptions are. As a result, the exempt activities are not clear.

✔ Members of the public and those who are not part of an organisation involved in LEDS should tick this box and complete the registration details.

Q11 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/Supplier] Don't know
☐	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).
☐	c.	N/A – please explain

Organisational preparedness

Thinking about your organisation, managers and users:

Q12 Does your organisation understand what new organisational measures may be needed to meet the requirements of the Code and Guidance Document?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
If you disagree, please let us know why				

Q13 How easily could your organisation comply with the Code?

Very easy	Easy	Neither easy nor hard	Hard	Very hard

Please explain where any further explanations would be helpful.

What other behaviours and responsibilities should be included?

What work would your organisation need to complete to become compliant?

Q14 Does your organisation currently produce a Data Protection Impact Assessment (DPIA) covering the activities in the Code?

Yes	No	Don't know

If yes, what does the DPIA cover?

If yes, is this DPIA published?	Published		Not published	
If published, is a web link available?	www.			

Q15 Do you think that the Code will help you to have improved access to data and services (for example, by enabling other organisations to share more appropriately)?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree

If you disagree, please let us know why

Q16 What other reports do you produce or publish covering the activities in the Code and Guidance Document?

Could you provide a copy or web link?	www.

Q17 What roles have been identified in your organisation to cover the responsibilities outlined in the Code and Guidance Document? If roles have not yet been identified, what is your implementation plan?

Q18 The College of Policing working with the Home Office are setting a national training requirement for the Code. Does your organisation understand the need to implement a learning and training requirement that goes alongside the Code and Guidance Document?

Yes	No	Don't know

If yes have you started to consider what you would need to do to implement the Code?

If no or don't know, how can this be made clearer?

Q19 What training, learning or guidance measures need to be implemented to support the ethical fair and diligent use of LEDS and who should provide this?

Q20 Does your organisation understand how to share data proportionately with other organisations, as required by the Data Protection Act (2018), and the measures needed to facilitate this?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree

If you disagree, please let us know why

Thank you for participating in this consultation.

About you

Please use this section to tell us about yourself.

Full name	
Job title or capacity in which you are responding to this consultation exercise (for example, member of the public)	
Date	
Company or organisation name (if applicable)	
Address **Postcode**	
If you would like us to acknowledge receipt of your response, please tick this box	
Address to which the acknowledgement should be sent, if different from above	
Redaction If you would like any answers to remain confidential, please indicate the reasons for this and the responses this relates to.	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

Contact details and how to respond

Please send your response by 09 September 2020 to:

Email: **LEDS.code@college.pnn.police.uk**

Complaints or comments

If you have any complaints or comments about the consultation process, please contact the College of Policing at the above address.

Extra copies

Paper copies of this consultation can be obtained from this address. The consultation is also available online at **https://www.college.police.uk/What-we-do/Standards/Codes_of_practice/Pages/Law-Enforcement-Data-Service.aspx**

Alternative format versions of this publication can also be requested.

Publication of response

A paper summarising the responses to this consultation will be published by 30 November 2020. The response paper will be available online at **https://www.college.police.uk/What-we-do/Standards/Codes_of_practice/Pages/Law-Enforcement-Data-Service.aspx**

About the College

We're the professional body for everyone who works for the police service in England and Wales. Our purpose is to provide those working in policing with the skills and knowledge necessary to prevent crime, protect the public and secure public trust.

college.police.uk

Follow us
@CollegeofPolice

C096I0620