Response

College of Policing consultation – Code of Practice for the Law Enforcement Data Service (LEDS)

About Unlock

Unlock is a national independent advocacy charity for people facing obstacles, stigma and discrimination because of their criminal record. Every year we hear from thousands of people who are unnecessarily held back in life because of their criminal record. We work at policy level to address systemic and structural issues. We listen to and consult with people with criminal records, undertake research and produce evidence-based reports to inform policy makers and the public.

About this response

Unlock welcomes the opportunity to provide a response to the College of Police consultation on the Code of Practice for the Law Enforcement Data Service (LEDS). This response sets out our answers to the questions that we have chosen to respond to, and accompanied to this is the consultation questions pro-forma to provide general details about our response.

Responses to questions

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.)

No, they do not. In using the range of answers provided in the consultation response, we would say we disagree with this.

Section 3.7 of the guidance document states that a list of organisations will be maintained by the Home Office and will be available online. The details shared as part of this consultation ("Organisations with access to LEDS" document) doesn't specify what information organisations have access to.

This does not meet two of the five aims – promoting accountability (which states: "The Code and the Guidance Document encourage transparency in how personal data within LEDS is used, managed and deleted") and promoting understanding (which states "Members of the public should feel reassured that the protections provided by the Code and the Guidance Document will help to preserve their data and privacy interests.") It is important to ensure that LEDS users see only the information relevant to their role and the purpose of an enquiry.

The guidance document dates that commercial organisations are "given limited access to redacted or filtered data for use in applications that support law enforcement purposes, such as checking for vehicle fraud." The published list of organisations should include details of what data they will have access to – for example, which "profiles" in LEDS do they see, and what level of information is available.

Although not the focus of this consultation, it should be made clear whether the organisations listed have been subject to a review of whether access to LEDS is appropriate and, if so, at what level). For example Cygnet Hospital Clifton and Edmonds Marshall McMahon (a private prosecutions firm) are listed as having direct access via ACRO – how was it decided that these organisations should have direct access and can other private firms also apply for access?

All data sharing agreements with organisations who have access to LEDS (directly or via others) should be published.

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

No, it does not. In using the range of answers provided in the consultation response, we would say we disagree with this.

Page 30 of the Guidance Document states: "Data that has been entered onto LEDS (or originating databases) should be accurate at the point of entry but new information may arise, for example a missing person may be found or an event may need to be added. This includes arrest, entry into custody, committal (or outcome of) court proceedings."

The Code does not state that users have a general responsibility to ensure data held in LEDS is of high quality; it only creates that duty when creating or amending a record. The rest of the time, users are not expected to take responsibility for quality, and so they are not required to update or improve records unless they had some other reason to amend them.

This leaves no-one responsible for records becoming out of date, as long as they were correct when created, and no-one responsible for noticing patently false information is circulating in the database.

The Code does require that users ensure data is high quality at the time that a record is created, as provision 8B of the Guidance Document ("Creating the data record on LEDS"). It may be intuitive to only require data be technically correct as of the moment it is input, but this does not reflect the reality of policing. Large amounts of data are time limited, or relate to pending processes which will at some point come to an end.

This means that users will necessarily input data which is only correct for a short time, but there is no specific duty for that user to return and "complete" these records unless something else prompts an amendment. This inevitably creates a factually incorrect record further down the line. The GDPR requirement to update records does not work if no-one is responsible for making the updates.

The responsibility for quality must not only apply when data is being inputted; it must be forward looking and require users to retain responsibility for a record and when necessary have a duty to ensure that it is properly and promptly updated.

The Code's emphasis on quality at the point of input also creates another problem for accuracy. It is assumed that if quality is properly maintained at input, there is no need for users to worry about the

credibility of data that they view. Users do not have a specific duty regarding the quality of existing data unless they are already actively amending it.

8C of the Guidance Document ("Amending and updating the data record on LEDS") requires that inaccurate records are corrected only "at the point that the inaccuracy is revealed", in accordance with GDPR requirements, but only defines inaccuracies in relation to other databases. Users do not have a duty to "notice" inaccuracies themselves. If a record is never cross referenced, it will stay inaccurate indefinitely.

The Code should include the duty to maintain quality at all times, not just when writing or amending records. Users cannot be expected to check in detail for each record, but they should not simply trust that the database is correct when it appears to them that data is faulty. We would hope that users already do undertake this work, but it should not be optional.

Unlock has come across many examples where information entered on to the Police National Computer has not been kept up to date. For example:

1. Police users recording conditional cautions as convictions (while the conditional elements are outstanding) rather than recording as a conditional caution or updating the record once the conditional elements have been completed. Details of the problems that this can cause are set out on our information site.
2. Court users not recording compensation orders as having been paid. For example, the case of Julian. Court users currently work on the basis of having no responsibility to record this, so LEDS (like PNC currently) will always be out on date on compensation orders. The DBS currently try to cover for this by not disclosing the conviction if they have receive proof of payment from the individual, but the systemic inaccuracy remains.
3. Court and/or police users not recording court orders of having ended. For example, the case of Toby.

The Code and Guidance Documents do not make it clear who has responsibility in situations like those listed above.

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?

We strongly disagree that the Code is clear on this.

Page 36 of the Guidance Document (section E – Review, retention and disposal of data on LEDS) does not provide details of the retention periods or set out the criteria for deletion.

In the "Why might my details be on LEDS" document, for those convicted or accepted a police caution, it states "the entry will remain on the database until you reach 100 years of age, although this is currently under review". This shows that the LEDS retention policy is not yet finalised but gives no timeframe for when it will be.

It is difficult for the Code of Practice and Guidance Document to be consulted on without the details of retention periods. The Home Office should consult with stakeholders, including Unlock, as part of the review of retention, and the outcome of this should be integrated in the Code of Practice and Guidance Document.

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

We strongly disagree that the Code and Guidance Document are clear on the types of activity that will be exempt.

The word “exempt” or “exemption” does not appear in the Code. The word “exempt” does not appear in the Guidance Document, and “exemption” only appears three times – all in relation to subject access requests.

The public guide

The public guide was not included in the consultation, however this is an important part of the puzzle. It is vital that this guide is shared with stakeholders in draft form so meaningful feedback can be sought before publication.

More information

Written	September 2020
Contact	policy@unlock.org.uk
Address	Maidstone Community Support Centre, 39-48 Marsham Street, Maidstone, Kent, ME14 1HH
Web	www.unlock.org.uk | @unlockcharity