College of Policing

Working together to prevent crime

Questionnaire for public consultation

Public consultation on the Code of Practice for the Police National Computer (PNC) and the Law Enforcement Data Service (LEDS)

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

Members of public and interested bodies are invited to answer the questions, having read the Code of Practice, guidance document and glossary provided.

Privacy notice

The information you have provided will be held by the College of Policing in accordance with Data Protection legislation. Your information will be lawfully held and processed for the purposes of informing the consultation phase of guideline development.

The information is processed under the lawful basis of public task.

The information you provide will only be used to inform development of the product.

Your information will be shared with internal business units when analysing feedback.

Your information will not be shared externally or outside of this process.

We will hold your information for one year. After this period your information will be securely disposed of.

The College takes its data protection responsibilities very seriously. Your information will be held securely and will only be processed for the purposes stated above or to fulfil a statutory obligation.

You have certain rights under the Data Protection legislation regarding your personal information, which includes the right to access information held about yourself, to ensure it is accurate and to ask it is deleted or no longer processed.

For more information about your rights please see our full privacy notice, which can be found on the legal page of our website. You can also contact our Data Protection Officer by emailing: **Data.Protection@college.police.uk**

Questions

Q1 The Code of Practice is a public document addressed to chief officers of police forces. The Code of Practice has been produced to:

a. **promote the lawful and fair use of the data and information managed within PNC and LEDS**
b. **ensure that chief officers adopt consistent and effective practices in using the information obtained from PNC and LEDS**
c. **support the ethical, fair and diligent use of information accessed from PNC and LEDS**

The Code seeks to do this by setting out ten principles for the ethical and professional use of the data and information that is managed within PNC and LEDS. Thinking about the intention of the Code, do you consider it to be a coherent and understandable document that provides clear direction to chief officers?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

If you answer disagree or strongly disagree, please indicate why.

Background
The Information Commissioner previously responded to the consultation on the LEDS Code of Practice and suite of documents in Summer 2020 and some of the comments which we provided then are still applicable to this consultation.

It should be noted that the Information Commissioner has access to data on the Police National Computer (PNC) through ACRO in order to support investigations as part of his regulatory functions. Our responses to this consultation are from the perspective of the data protection regulator in monitoring and enforcing compliance with data protection law.

Not all of the questions are relevant to the Information Commissioner, so these have been left blank, alongside the agree/ disagree boxes.

Technical capabilities of the Police National Computer (PNC)
The Code has been amended to include the PNC. The PNC will need to have functionalities that allow controllers accessing it to conform to the principles of the Code and be compliant with

obligations set out in data protection law. The Information Commissioner would welcome information about how this is ensured, and also that this is being communicated to other stakeholders.

The structure of the documents
Data protection requirements and considerations apply in all principles of the Code. While the Information Commissioner appreciates that the ten principles and the steps outlined in the Code have been developed in a way which is familiar to the users of the systems and follow the life cycle of data processed, this means that the way data protection principles are currently presented is repetitive. In particular, 6.3, 6.4, and 6.7 of the Code (pages 13-14) make reference to the importance of the accuracy of data held.

Because of the way it is currently presented, there is a risk that users may overlook that data protection considerations apply across the piece – i.e. if accuracy is not mentioned in the other Code principles, users may think it does not apply. This also applies to the list of bullet points which outline the responsibilities of each person based on their role (Chapter 3 of the Part B guidance) – if compliance with an aspect of data protection law is not explicitly listed, this may be missed. To address this, the College would need to ensure that Chapter 3 of the Part B guidance is comprehensive and addresses all the data protection compliance requirements.

It would also be useful to reiterate the applicability of data protection law to all the ten principles set out in the Code. Clarity on the application of data protection law will avoid confusion for controllers, recognising that there is convergence in the frameworks.

Governance and accountability

We would suggest that the Code principle on accountability and audit is expanded to highlight other governance considerations around Data Protection Impact Assessments (DPIAs), Data Protection Officers (DPOs) and logging requirements under the Data Protection Act (DPA).

Q2 The guidance document has been produced in two parts to better inform organisations that use PNC and LEDS how to comply with the Code. Thinking about the two parts of the guidance document, do you consider that they provide sufficient detail to enable police forces and other organisations that use PNC and LEDS to comply with the principles set out in the Code?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

If you answer disagree or strongly disagree, please indicate why.

Click or tap here to enter text.

Q3 Do you feel that, taken together, the three documents (the Code, Part A and Part B of the guidance document) effectively support public confidence in meeting the five

aims that are outlined on page 7 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 answer disagree or strongly disagree, please indicate why.

Click or tap here to enter text.

Q4 Do the Code and the guidance document provide clear guidance to police and other organisations who might be using PNC and LEDS as to how those organisations should store, use, manage and dispose of the data processed through these systems?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

If you answered disagree or strongly disagree, please let us know why.

Click or tap here to enter text.

Q5 Thinking about privacy laws and regulations, to what extent do you consider the Code and guidance document to have clearly set out the performance expectations and behaviours for organisations that use PNC and LEDS?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

If not, are there other sources of advice, guidance or specific legislation that should be cited?

Data protection legislation

A consistent reference to Part 3 of the DPA will assist users in locating the relevant part of the DPA which applies to criminal law enforcement processing. There should be clarity that other processing, such as civil enforcement, will fall under the UK GDPR and its requirements.

Controllership of the system
The Information Commissioner appreciates the prominence given to data protection in Chapter 5 of the Part A guidance, but there are a number of areas which require review and clarification.

The Information Commissioner has previously provided feedback that the complex network of relationships between organisations which provide data to and access data from national policing systems should be clearly mapped out so it is evident whether organisations are controllers/ joint controllers/ processors.

In our response to the LEDS Code of Practice consultation in 2020, we highlighted the following:

The Information Commissioner is of the view that further clarity can be provided on the following:

Controllership

This was an area which the Information Commissioner has raised previously, where due to the number of actors which have access to LEDS, it was important to outline very clearly what the relationships were in terms of data protection obligations. In the documents, there are several references of joint-controller agreements or arrangements and it would be useful to clarity what these mean. Not all user organisations would be joint controllers and it is unclear in some circumstances whether this refers to data sharing agreements. The use of this term needs to be explained, and applied consistently, so readers are aware what it refers to.

There are a number of relationships outlined in data protection legislation, such as:

• Joint controllership where more than one controller get together to jointly determine the means and purposes of processing. Organisations may be joint controllers for certain data sets if they jointly decide the purpose for processing, but may not be for other data sets. For e.g. the Home Office may be joint controller with the NPCC (representing the police forces) for certain aspects of LEDS but may be sole controller of data processed for immigration purposes. If two or more controllers are joint controllers, then a transparency agreement between joint controllers will have to be in place in accordance with Article 26 of the GDPR and section 58 of the DPA 2018. Our guidance has more information: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/

• Other organisations given access to LEDS may be separate controllers, in their own right, processing data on LEDS for their own purposes (i.e. controllers who are not in a position jointly with the police forces to determine the means and purposes of processing the data on LEDS). We strongly recommend that data sharing agreements (where there is personal data exchanged between different data controllers) should be in place.

• Controller-processor agreements also need to be in place for those processing on behalf of controllers and these would need to meet the requirements of data protection legislation.

It's really important that the different relationships are clearly defined and the documents updated accordingly to clarify whether every reference to joint-controller agreements refer to transparency agreements, data sharing agreements, or something else.

In the current consultation, it is not clear in sections 5.2.4 and 5.2.5 of the Part A guidance whether forces retain controllership of data submitted to the PNC and LEDS. It is important that the appropriate agreements and contracts are in place and it is unclear in the context of the guidance documents whether 'data processing contracts' refer to the controller-processor contracts which need to be in place in accordance with data protection law.

The current draft of the documents does not make the controller/ joint controller/ controller-processor relationships clear. In particular, the roles of the NPCC and the Home Office require further consideration. The description of the Home Office and NPCC providing governance and leadership in sections 4.2 and 6.3 of the Part A guidance suggests a more central role for both organisations where they could be controllers. Pages 30 and 43 of the Part B guidance, which mention the Home Office removing/ restricting organisational access and "ensuring that joint-controller arrangements, data-processing contracts or memoranda of understanding clarify whether organisations will either directly access all functionality on LEDS or will gain access to restricted data sets", again appear to suggest that they will be determining, to a certain extent, the means and purpose for processing data.

Setting out the relationships clearly would ensure that the respective roles, responsibilities and liabilities in data protection terms are fully accounted for and this will make it easier to facilitate the exercising of data subject rights.

Data quality principles
The Information Commissioner welcomes the focus on data quality standards. As previously commented on, the data minimisation, accuracy and storage limitation principles in data protection law govern the quality of data and the lack of compliance with one of the principles is likely to mean non-compliance with the rest. The Code and guidance documents could benefit from drawing out the inter-relatedness of these principles and how this impacts on data quality. In particular, while accuracy and retention have dedicated Code principles, greater emphasis should be given to the data minimisation principle.

Data subject rights
The onus is on controllers to ensure that their processing of personal data complies with data protection legislation and that they can demonstrate compliance. For example, under section E of the Part B guidance, it should be clear to users that regardless of whether an individual exercises their right to erasure, controllers have to ensure that retention of data complies with the data protection principles and should actively review and ascertain whether ongoing retention of personal data is justified. See section 47 of the DPA for more information.

Q6 Do you agree that compliance with the Code would ensure that data held in PNC and LEDS will be of the highest possible quality, accurate and current?

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

If you answered disagree or strongly disagree, please let us know why.

Click or tap here to enter text.

Are you answering:

☐ As an interested individual acting in a private capacity (for example, someone providing their views as a member of the public)

☐ As an individual acting in a professional capacity

☒ On behalf of an organisation

☐ Other

If you are representing an organisation with an interest in the management and application of PNC or LEDS, please specify the name of your organisation:

Information Commissioner’s Office

☐ Please tick if you want us to treat your response as confidential.

Thank you for participating in this consultation.

About you

Please use this section to tell us about yourself.

Full name	Wei Lynn Ng
Job title or capacity in which you are responding to this consultation exercise (for example, member of the public)	Senior Policy Officer High Priority Inquiries – Policy Projects
Date	20/04/2022
Company name or organisation (if applicable)	Information Commissioner's Office
Address **Postcode**	Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Click or tap here to enter text.
If you would like us to acknowledge receipt of your response, please tick this box	☒ (please tick box)
Address to which the acknowledgement should be sent, if different from above	Click or tap here to enter text.

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.

Click or tap here to enter text.

Contact details and how to respond

Please send your response by 21 April 2022 to:

PNC and LEDS Code of Practice Consultation Team, College of Policing

Email: [insert email address]