

Consultation on the

Police Information and Records Management

Code of Practice

Feedback form

Consultation closes 8 March 2021

# About this consultation

We want your views on our Police Information and Records Management Code of Practice.

The Code applies to the police forces maintained for the police areas of England and Wales as defined in section 1 of the Police Act 1996 (or as defined in any subsequent legislation). It also relates specifically to chief officers in the discharge of their functions. The code also has relevance for anyone working in forces particularly those working in the area of Information Management.

The new Code of Practice extends the MOPI Code of Practice 2005 to include corporate records as well as policing records. It also updates the requirements in line with General Data Protection Regulation and the Data Protection Act 2018.

Please use this form to send us your feedback. The feedback boxes will increase in size as you enter your text.

Your completed form should be emailed to I&RMgtCode@college.pnn.police.uk**.** Please respond no later than 8 March 2021.

 All feedback will be collated and analysed by College staff for and the draft Code of Practice amended if appropriate. We will only contact you if we need to clarify any of your comments and you give us your contact information. A summary of changes made as a result of feedback will be published at the same time as the final APP.

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

Your personal 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.pnn.police.uk

## About You

|  |  |
| --- | --- |
| Name (optional) | *Dr Ksenia Bakina and Matthew Rice* |
| Role (optional) | Click here to enter text. |
| Organisational (optional) | *Privacy International (PI) and Open Rights Group (ORG)* |
| Please tell us if your views are personal or whether they represent an official response from your organisation. If official please state in what context (e.g. Chief Constable, Head of information) | *The responses below represent an official response from Privacy International and Open Rights Group* |
| if you are willing to be contacted should we need further clarification on your comments, please provide your contact details | *kseniab@privacyinternational.org**,* matthew@openrightsgroup.org |
| If you wish to be informed when the final Code of Practice is published, please provide your contact details | *kseniab@privacyinternational.org**,* matthew@openrightsgroup.org |

### Consultation Questions

**It will be helpful for us to understand why you have given a particular answer, or how you think the Code could be improved. Please provide detailed comments wherever possible.**

|  |
| --- |
| 1. To what extent do you think the Code is easy to follow and understand? Please let us know if there are any specific changes that you would like to see. Whilst the Code is clear in terms of layout and language, the actual information provided about the management of police information should be expanded. Transparency is key and there is a need to address the reality of policing in the 21st Century and the ongoing real-time use of massive databases in the modern age. Policing in the UK and around the world has turned into a sophisticated data operation.Privacy International (PI) and Open Rights Group (ORG) believe the obligation of transparency, where relevant, be imposed by the General Data Protection Regulation and Data Protection Act 2018 should extend to all organisations and relevant third parties with whom the police information and records will be shared and who will have access to this. Further, concrete information is needed in the final Code around the safeguards that will be implemented, how access will be allocated and reviewed in the future, who will oversee this process and the extent to which records and police information will be shared with other organisations and third parties.The code is currently too vague and does not provide sufficient information about how the relevant measures will be implemented. For example, it is not clear what specific safeguards will be adopted in relation to the management of data and how long the data will be kept. Also, the effect of the Code’s wider definition of policing purpose than the one given in the Data Protection Act 2018 must be expanded for its effect on:- Legal basis for processing- Processing of special category data- Rights of the data subject- Responsibilities of the data controller and processors- Archiving and preservationWhilst the Code provides that metadata should be kept for as long as it is required, it doesn't provide for the safeguards outlining how this will be determined or when metadata and other records must be deleted. 2. Do you believe it is clear what forces will need to do as a result of the Code?It is not entirely clear what the forces will need to do because the Code fails to fully explain how they need to incorporate the principles in their work. The Code is ambiguous and does not explain in any real detail how the relevant principles and obligations will be achieved or implemented. The Code should be expanded to provide further clarity and instruction.We believe the way police records and information are managed, stored, recorded and disposed of can pose serious threats to privacy and other fundamental rights, and therefore must not only be subject to strong oversight, safeguards, and transparency measures, but also that these measures must be clear and implementable, with direct lines of responsibility. At the moment, the Code does not provide this, and instead largely refers to broad principles rather than concrete measures.3. To what extent do you think Section 5, ‘Organisational requirements’, is easy to understand and presents the issues that forces will need to address in order to deliver the code? Please let us know if there is any specific information that needs to be added. Whilst we are pleased that there is emphasis on training of the relevant staff in Section 5 and identifying key posts required for the management of police records, more could be said about who will be overseeing this training and such roles. More detail is required to outline how the training will be implemented and what safeguards will be adopted to ensure that staff are applying the relevant training to the police records and using the information systems appropriately. Also, the Code of Practice needs to provide if any auditing will take place to ensure compliance with the Code and relevant legal frameworks. More detail is required about how auditing will be undertaken and at which intervals. Currently, it is not clear how the accuracy of information will be checked and by who. Further, the Code of Practice fails to provide what safeguards will be adopted to protect the police records from system failure and other risks, such as hacking or ransomware. 4. To what extent do you think Section 6, ‘Information Sharing’, is easy to understand and provides a ‘high-level’ statement of the factors that need to be considered when sharing information? Please let us know if there is any specific information that needs to be added. Section 6 is rather confusing and is not easy to understand. This is because section 6.3. states that sharing of the information between police forces is subject to constraints outlined in 6.16 of the Code. However, paragraph 6.16 is missing from the code. As a result, the Code fails to make clear what constraints will exist to ensure that sharing of information between police forces is appropriate. It is also unclear what safeguards will be implemented to ensure that sharing of information between various police forces is lawful, proportionate and reasonable. The Code does not mention any circumstances under which information should not be shared. It also fails to address whether any role-based access controls will be implemented to ensure that the information is not shared beyond its purpose, including but not limited to those police officers and/or organisations who should not have access to this.The code at paragraph 6.4 states that the Chief Officers will ensure that the police force seeking access to the information applies the principles set out in this Code, but the Code fails to explain how will this be done. If it’s a matter of police forces completing the relevant training, that in itself may not be sufficient to ensure that they are complying with the code.Part 6 of the code also states that Chief Officers will share information with bodies other than police forces in England and Wales. However, the Code fails to specify with which organisations the information may be shared and what safeguards will be put in place to insure that the sharing of information is appropriate, lawful, proportionate and reasonable. Whilst section 6.9 does state that Chief Officers should have regard to any national guidance or Code and any protocols that may be relevant, this is too broad to be of any substantive use. The code should specify which guidance and protocols Chief Officers refer to and what type of safeguards should be implemented in order to comply with these.It is also unclear what safeguards will exist when the information is shared with other bodies. This is concerning, considering the ICO report on mobile phone extractions issued in June 2020 was very critical of the way information is managed and shared.Further, Section 6.7 states that: “In cases where information is shared on a regular basis, where there is a legal basis to do so, formal arrangements should be made through the development of data-processing contracts, memoranda of understanding (MOUs), service-level agreements (SLAs) or information- sharing agreements.” This section must be revised to outline what safeguards apply to information shared on a non-regular basis, what constitutes a “regular basis”, and be clear that the relevant agreements should be made publicly available.Whilst section 6.10 mentions that chief officers must apply the criteria contained in sections 72-78 DPA 2018, that in itself is not sufficient information to ensure that chief officers understand what the criteria means or how to apply it in practice.5. To what extent do you think the principles of the code are appropriate and provide a clear framework to assist forces and individuals with managing their information? Please let us know if there is any specific information that needs to be added. The principles, whilst useful, are too vague to be able to sufficiently assist forces with managing information. The main concern is it’s unclear how these principles will be achieved and observed. For example, whilst paragraph 4.4. of the Code mentions that police forces must have appropriate governance arrangements for information in place, it is silent about what these arrangements should look like. This is an important consideration for the Code, especially for sensitive processing under Part 3 of the Data Protection Act 2018. The Data Protection Act 2018 at section 35(4) sets out that sensitive processing can only occur under narrow cases, one being the consent of the individual, the other being where an “appropriate policy document” is in place. [<https://www.legislation.gov.uk/ukpga/2018/12/section/35/enacted>]. Section 42 of the DPA18 expands on the meaning of “appropriate policy document” and the Code would benefit from including those requirements [<https://www.legislation.gov.uk/ukpga/2018/12/section/42/enacted>]. The Code does not provide what are the appropriate organisational and technical measures required in order to comply with the Code.Further, whilst paragraph 4.7 of the code states that Chief Constables should ensure that access and retention is legitimate, it is unclear how this will be achieved and what kind of steps will need to be taken to achieve this. However, we do welcome the emphasis on ensuring forces do have the legally required data protection impact assessments (DPIAs) and equality impact assessments (EIAs) in place when processing personal and sensitive personal data. We recommend that both the DPIAs and the EIAs will be subject to public scrutiny and consultation process.We are also pleased to see emphasis on transparency and that records need to stand up to scrutiny and to meet legislative and regulatory requirements, including individual rights and entitlements. However, again, it is not clear how this will be achieved and how the forces will be able to demonstrate compliance with the principle of transparency.There is a potential tension with the commitment to transparency. The Code acknowledges that Part 3 of the DPA 2018 does not include transparency as a principle for law enforcement processing, and goes on to say that police forces must ensure they fulfil their legal data protection and freedom of information obligations. One of the key legal obligation under Part 2 DPA 2018 related to transparency is data subject rights found in section 45 of the DPA 2018. While the controller may restrict the rights of a data subject for a number of reasons under section 45(4) there is a corresponding obligation to inform the data subject of the restrictions under section 45(5). The Code would benefit from reflecting that legal responsibility. The tension we foresee exists at 4.27 of the Code where it states that “where possible” the existence of the asset (which we understand to mean a record held reflecting para 3.5 of the Code) should be “publicly known”. This is a useful principle for data subjects in particular to exercise their right of rectification of an asset that may be inaccurate. The “publicly known” principle may be able to let an individual make an educated assessment as to the information being processed and to correct it if it is in error. However, the restrictions of transparency set out in section 45(5) of the DPA2018 could render the “publicly known” principle empty. The Code should provide guidance on how forces should balance these two potentially competing principles in a way that is equitable to data subject rights and accountability of the management of police information.Further, whilst the code refers to the obligations to dispose of information, it is not clear how this will be done and the guidelines for this are vague. Paragraph 4.28 states that information and metadata must be suitably secured and stored, managed, handled, maintained and disposed. However, it is not clear what safeguards will be adopted in order to ensure that the systematic failures that have been previously highlighted in the ICO report dealing with the use of mobile phone extraction are avoided. [<https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf>] The ICO report highlighted numerous risks and failures by the police in terms of data protection and privacy rights. The report also confirms PI’s concerns that the data extracted and processed from the mobile phones was often too excessive. The police and the CPS were not giving enough consideration to necessity, proportionality and collateral intrusion. Additionally, whilst paragraph 4.31 provides that access to information must only be allowed to authorised individuals who need access for their lawful function, it is not clear what safeguards will exist to ensure that information is not revealed to unauthorised individuals. This is particularly concerning in light of LEDS role-based access controls and information being shared with outside organisations. It is unclear how the information containing personal data of individuals will be safeguarded against deliberate misuse of their data, such as so-called LOVEINT - the use of massive and intrusive databases to spy on partners [<https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/> ], or from incorrect or invalid data. As a result, the Code does not explain in sufficient detail how they will be safeguarding people, promoting accountability and understanding.The Code of Practice fails to provide concrete safeguards to ensure these practices do not take place, nor outline details of the redress or disciplinary procedures as a result of misuse. It is also not clear whether, as we have seen in various disciplinary proceedings before Professional Standards in the Met, disciplinary proceedings may be bypassed altogether by officers under investigation leaving their roles [<https://www.telegraph.co.uk/news/uknews/law-and-order/9839944/200-officers-a-year-retire-or-resign-to-avoid-disciplinary-proceedings.html>]There is a need for clarification at Principle 6. At 4.36 where a decision is made to retain a record for longer, there are circumstances in which it requires more than just a justification and designation, but also a need for approval from an independent body under the Protection of Freedoms Act 2012 [<https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted>] . The definition of “record” includes biometric materials. But this principle fails to reflect that where there is no power to retain a person’s biometrics, but a Chief Officer of police decides that for reasons of national security they should be retained he / she can do so by making a National Security Determination which the Biometrics Commissioner is required to examine to ensure they meet the legal tests required. Additionally, where the police in England and Wales have arrested but neither charged nor convicted a person, they cannot generally keep the biometrics that they took from the person on arrest. However, for certain more serious offences the police can make an application to the Biometrics Commissioner. Currently, the Code just states that the justification for retention should be recorded. However, it must not only be recorded, bur also, in some circumstances, in particular relating to biometric material, it should be reviewed and approved by the Biometrics Commissioner. The Code must reflect that need for independent oversight.Further, principle 7 which deals with disposition of records also fails to provide what safeguards will be implemented to ensure that relevant data is appropriately disposed of and if an IT system does not have a delete functionality, what safeguards will be implemented that data risks are avoided. Ultimately, while the principles are useful, they are insufficient as safeguards for users and organisations to ensure their compliance with the ethical standards, human rights and equality principles. Numerous reports recently highlighted serious problems surrounding the way Police are managing their records, from accidental deletion of records (<https://www.theguardian.com/politics/2021/jan/15/priti-patel-under-fire-as-150000-police-records-accidentally-lost>) to failures to inform relevant EU countries that their citizens have been convicted of murder in the UK (<https://www.theguardian.com/law/2021/mar/02/uk-failed-to-inform-eu-countries-about-almost-200-killers-and-rapists?CMP=Share_iOSApp_Other>). Considering these issues, it is imperative that the Code of Practice provides concrete safeguards to ensure these practices do not take place.Finally, the Code is deficient in reflecting to individuals the opportunities for management of their information in failing to articulate all the processes available for individuals. In 2017 the Home Office established a custody record deletion process following the 2017 Custody Image Review. People whose biometrics are being lawfully retained by the police can apply for the ‘early’ deletion of their records from national policy systems, namely the Police National Computer, the National DNA Database and the National Fingerprint Database. This is referred to as the Record Deletion Process. This process is relevant to records held on PNC, NDNAD and IDENT1 to which this Code is supposed to be considered in conjunction. It is unclear why the Record Deletion Process is not even acknowledged and we suggest that such notification is given in this document to other processes for individual rights and police information.6. To what extent do you think that the Code sufficiently covers the relevant data protection safeguards? Please let us know if there is any specific information that needs to be added.Whilst the Code references various data protection principles, such as requirement for the processing of data to be lawful and fair, it lacks detail about how these principles will be achieved in practice. Whilst it emphasises that forces must adhere to the legal data protection obligations, it doesn’t provide the details about what steps need to be taken and what safeguards implemented in order to comply with these obligations.At the moment it is not clear who will be checking the compliance of the forces with the data protection principles and how often these should be checked. The code leaves it largely up to each individual police force to put the relevant arrangements in place, which could lead to misunderstanding of the principles, what needs to be done to comply with them and disparities about how the information is managed from one force to another.We are also concerned that the code in paragraphs 3.8 and 3.9 provides a wider definition for policing purpose than that which is given for law enforcement purpose in part 3 of the DPA 2018. Part 3 DPA 2018 defines the law enforcement purpose as ‘the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’. However, policing purpose in the code additionally includes preservation of order, protection of property and any police duty or responsibility arising from common or statute law.Whilst the Code does state in paragraph 3.10 of the Code that some information may be processed under Part 3 of the DPA 2018 and other information under part 2 DPA 2018, it is not explained how this will work in practice. This would need to be explained in much more detail and the Code also needs to provide an explanation as to why the policing purpose is interpreted much broader than the law enforcement purpose under Part 3 DPA 2018.7. To what extent do you think compliance with the Code will support public confidence in the way forces manage their information and records? Please let us know if there is any specific additional content that could help us.We believe that the broadened definition of 'policing purpose' risks providing data that goes beyond law enforcement purposes‚ as provided under the DPA 2018 may confuse the public without clear communication setting out the effects of this. Under data protection law, fairness is intimately linked with an individuals’ reasonable expectations as to how their data may be used. Thus, the way data is increasingly used for 'policing purposes' and the sources where it may come from, may not be within individuals’ reasonable expectations because they are either unaware of it or because they are aware of it but find it unacceptable, thus raising questions of fairness. This may decrease public confidence in the way forces manage information and records. Particularly, since there is no justification provided for the wider definition of 'law enforcement purpose' than what is provided under the DPA 2018. Further, considering the general vagueness of the Code as discussed above, it fails to provide sufficient transparency which will not lead to an increase in public trust.8. Do you have any comments on potential positive or negative impacts of the Code on individual members of the public? There are currently about 12 million images enrolled into the PND gallery - equivalent to 1/5th of UK’s population, a number of which are held unlawfully. The legality of the retention of custody images was challenged and in a 2012 judgment the High Court held that the continued retention of images from unconvicted individuals under the Metropolitan Police Service’s policy for the retention of custody images, which followed the Code of Practice on the Management of Police Information and accompanying guidance was unlawful without case by case consideration.[<https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf>]. Considering the judgment decided that the real matter of concern, was not the Police failure to apply the guidance but the terms of the guidance itself, there is a need on the MoPI guidance to be clearer and firmer in its operation to meet the terms of the judgment and avoid the deficiencies that were found in the 2012 judgment.PND also has facial matching capabilities which enable users to upload a probe image from an external source, such as from CCTV, mobile phones, cameras, and photocopied documents such as passports. It then compares this probe image across all images attached to personal or custody records to see if there are any suggested matches. We are concerned that individuals whose information is contained may not have any knowledge that such an entry exists, let alone be able to correct any mistakes, accidental or otherwise. We strongly recommend the implementation of a robust system of redress to allow individuals to challenge their inclusion in police records and relevant databases (PND/PNC/LEDS) if they fear it to be unlawful, as well as sufficient transparency to allow individuals to understand if they are included.In particular, the ICO had significant concerns regarding the data entered into the Gangs Matrix database [<https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf>] Statistics from July 2016 show that 87% of the people recorded in the Gangs Matrix were from Black, Asian or Minority Ethnic (BAME) backgrounds. Further, 78% were Black, despite the fact that only 13% of London's total population are Black. Additionally, 99% of people recorded on the Gangs Matrix were male. The Code of Practice on the Police Information and Records Management needs to have safeguards in place to avoid such failures in the future. 9. How easy or difficult do you think it will be to implement the Code across forces?We believe it would be quite difficult to achieve consistency of implementation of the Code across forces because the Code is vague in many places and leaves a lot of crucial decisions to the forces themselves. As a result, this could lead to numerous inconsistencies between forces as to how the code is applied and how the safeguards are implemented10. Do you have any suggestions that you think would help the implementation of the Code?Given the risks of misuse and exploitation of data, we believe:* There should be clearer rules, providing clarity and foreseeability about when, why and how the police and other third parties are able to manage, record, store and dispose of police information and records.
* Robust policies and procedures must be put in place to ensure the appropriate handling and deletion of data. These policies should include oversight procedures and what safeguards will be adopted to ensure that the handling and deletion of data is compliant with data protection legislation.
* More transparency surrounding the way access controls and relevant authorisation will be assigned, controlled, monitored, and publicly notified.
* To meet the standards required for fair processing, there should be further guidance on how police forces should engage with individuals whose data has been stored on various databases (PNC/PND/LEDS) and to inform them about what their rights are.
* Details of how the APP is to be enforced should be made clear, including details regarding the redress or disciplinary procedures as a result of misuse of records or police information.
* More information should be provided to police officers, oversight agencies and the courts regarding the legal status of the APP and whether its provisions are binding or if they can be used as evidence within disciplinary procedures.
* Individuals need to be clearly informed about how they can exercise their data rights, and how to seek redress, including via an easily accessible online portal.

11. Do you have any other comments on the draft Code?Click or tap here to enter text. |

Your completed form should be emailed to **I&RMgtCode@college.pnn.police.uk**.

About the College

We’re the professional body for the police service in England and Wales.

Working together with everyone in policing, we share the skills and knowledge
officers and staff need to prevent crime and keep people safe.

We set the standards in policing to build and preserve public trust and we help
those in policing develop the expertise needed to meet the demands of today
and prepare for the challenges of the future.

college.police.uk