Public consultation: Code of Practice and Authorised Professional Practice

About defenddigitalme

defenddigitalme is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. We advocate for children's data and digital rights, in response to concerns about increasingly invasive uses of children's personal information. Funded by the Joseph Rowntree Reform Trust Ltd.

Contents

Question 1. To what extent do you think the Code is easy to follow and understand? 2
A fit-for-purpose test 3
Question 2. Do you believe it is clear what forces will need to do as a result of the Code? 3
Taxonomy cannot be optional in consistent national standards 4
How might forces reconsider their role in personal data and policing records 5
Data subjects as rights holders and implications for duty bearers 6
Question 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? 7
Question 5. To what extent do you think the principles of the Code are appropriate and provide a clear framework to assist forces and individuals managing their information? 7
Principle 3: Quality 8
Principle 4 Compliance 8
Principle 5 Accessibility 8
Principle 6: Review and Retention 8
Consistency across forces and decisions is easy on the easy things 9
Principle 7 Disposition 10
Question 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? 10
Data sharing registers 11
Distribute access not data 11
Data linkage 11
Question 6. To what extent do you think that the Code sufficiently covers the relevant data protection safeguards? 12
Question 7. To what extent do you think compliance with the Code will support public confidence in the way forces manage their information and records? 14
Question 8. Do you have any comments on potential positive or negative impacts of the Code on individual members of the public? 15
Question 9. How easy or difficult do you think it will be to implement the Code across forces? 15
Question 10. Do you have any suggestions that you think would help the implementation of the Code? 16
Question 11. Do you have any other comments on the draft Code? 16
Other related legislation 16
The Common Law Duty of Confidentiality and records of deceased persons 16

1. **Question 1. To what extent do you think the Code is easy to follow and understand?**

1.1. The purpose of the Code is to replace the Management of Police Information (MoPI) Code of Practice 2005. There is little here that suggests an appreciation of the significant changes in data processing as a result of the adoption of emerging technology over those fifteen years. Or that recognises what is new in revised data protection regimes, or changes in public attitudes or social and cultural changes.

1.2. The approach is outdated in terms of understanding what data is, where it is created, is stored and by whom on behalf of policing, and what good practice would look like. Retro-fitting a Code of Practice onto existing practice based on revising core 2005 wording, will not bring about its aims of improved practice.

1.3. To offer Forces a meaningful guide to good practice, the Code must demonstrate a thorough understanding of and address the various aspects of modern policing and data processing.

1.4. The Code must first recognise and address the necessary and concrete changes of policing practice in practical terms —much has changed since 2005 in the adoption of technology or legislation that results in data processing and with high-level impact on the everyday life of UK residents, involving surveillance of *non-criminal* activity at scale, such as the use of drones at public events,[1] facial detection or recognition in public places[2], or IMSI catchers[3], and the Prevent duty introduced in the Counter-Terrorism and Security Act 2015— and in addition the types of technology and where it is used are being expanded such as location monitoring GPS tags deployed after prison release on domestic violence offenders, or the use of biometric fingerprint readers[4] in roadside stops and stop-and-search.

1.5. The Code is missing any guidance to Forces on using data processing technology procured or adopted by police for data evaluation or analysis, such as in the creation of 'heat maps', data analytics, predictive algorithms, profiling and automated decision-making, the use of machine learning and artificial intelligence, facial recognition or facial detection tools processing datasets of photographs already held.

1.6. The Code should offer guidance to the Police when procuring third-party services that involve data processing on behalf of police. What are the quality, health and safety, ISO and other standards that should apply to any data processing devices and the companies that sell them or operate them on behalf of any aspect of law enforcement? Who is responsible for the data that those devices or activities create, do police forces consider those as 'police records' at all under the Code if those data remain on vendors' servers?

1.7. There needs to be a thorough understanding of the role of Controllers and Processors, and guidance could make recommendations for example that all vendor agreements should contain explicit clauses on data accountability, registers of use by the third-party employees or others as appropriate, and transparency.[5] i.e. consider how all of the Code will be adopted by a third-party processor, not only Forces themselves.

[1] The Guardian (2021) Drones used by police to monitor political protests in England https://www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion
[2] UK Authority (2020) South Wales Police lose facial recognition appeal case https://www.ukauthority.com/articles/south-wales-police-lose-facial-recognition-appeal-case/
[3] Computer Weekly (2020) Police secrecy over 'IMSI-catcher' mass surveillance of mobile phones https://www.computerweekly.com/news/252485535/Police-secrecy-over-IMSI-catcher-mass-surveillance-of-mobile-phones
[4] Wired (2020) Police use of fingerprint scanners disproportionately targets Black Britons https://www.wired.co.uk/article/police-fingerprint-scan-uk
[5] The UK DPA 2018 Meaning of "controller" and "processor" https://www.legislation.gov.uk/ukpga/2018/12/section/83/enacted

1.8. This Code feels too theoretical with little meaningful help to enable Forces to create their own Records Management Codes of Practice at local level fit for the real world.

1.9. A fit-for-purpose test

If it is fit for purpose, the Code should be able to demonstrate how it will achieve its aims to provide "*a framework to support a cohesive, ethical, effective and lawful approach to the management of information and records within the police service"*. Its test should be to state how this Code would address data related, well-known issues that have not met '*ethical, effective and lawful'* practice e.g.

1. Abuse of deceased children's personal data and identities by undercover police officers.[6]
2. The Gangs' Matrix without Equality Impact Assessment that "*does not clearly distinguish between the approach to victims of gang-related crime and the perpetrators, leading to confusion amongst those using it, or serious breaches of data protection laws with the potential to cause damage and distress to the disproportionate number of young, black me*n."[7]
3. Breaches of law on communicating rights and failure to meet Subject Access obligations.[8]
4. Mass deletion process security and audit safeguards.[9]
5. Data created or processed unlawfully through the use of emerging technologies.[10]
6. Children's rights are ignored in what is described as a consensual programme, Prevent, but where personal data is not managed on the basis of consent and retention is excessive.[11]

If these examples of practice could continue or be repeated under the Code, then it does not meet the test of paragraph 2.2. of "*improving accountability and increasing the public's confidence in the way that their information is managed*." And it would be unlikely that it provides the necessary "extra safeguards" as claimed in paragraph 3.11 to be, "*reflected in this code and supporting national guidance."*

2. Question 2. Do you believe it is clear what forces will need to do as a result of the Code?

No. Changes in technology, practice and legislation since 2005 require more significant amendment to the 2005 Code than this revised version offers and it is a welcome opportunity that the outdated Guidance could be substantially improved.

2.1. How should forces understand how this relates to practice on the ground? What would forces do differently in our case studies 1-6 as a result of the revised

[6] The Guardian (2020) Met faces legal action over spies' use of dead children's identities https://www.theguardian.com/uk-news/2020/dec/07/met-police-legal-action-spies-use-dead-childrens-identities
[7] The ICO (2018) ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/
[8] The ICO (June 2019) Enforcement notices served against the Met Police Service under the 1998 and 2018 Data Protection Acts for sustained failures to comply with individuals' rights in respect of subject access requests. And https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-supporting-people-accessing-their-data-from-the-police/
[9] BBC (January 2021) Police probes compromised after computer records deleted https://www.bbc.co.uk/news/uk-55684320
[10] BBC (2020) Facial recognition use by South Wales Police ruled unlawful https://www.bbc.co.uk/news/uk-wales-53734716
[11] The Guardian (2019) Family wins fight to delete child from Met anti-radicalisation records https://www.theguardian.com/uk-news/2019/dec/19/family-wins-fight-to-delete-child-from-met-prevent-anti-radicalisation-records

Code? If this is not clear, then guidance is not clear enough in the Code.

2.1.1. In some parts, the Code suggests a scenario, in *'Obligations of those receiving police information*' but then gives no guidance. For example, there is no guidance on what officers should do if a data subject makes a request to correct a record. Should only the accurate data be retained? Should both records be retained? What explanation for the correction should be added?[12] How will this affect national datasets or reporting if the national LEDS database has been uploaded from the original data? This is not clear from paragraph 6.13.

2.1.2. Principle 2 in the Code is particularly unclear what forces are expected to do as a result. The second principle "transparency" is confusing because different or conflicting ideas are conflated without any further guidance. *"4.13 Transparency should not overrule necessary operational and personal confidentiality. 4.14 Forces must be clear, open and honest with people from the start about how and why their personal data is being processed. 4.15 The first data protection principle, set out in Part 3 of the DPA 2018, requires that processing is lawful and fair. ...* ***it is recognised that this may prejudice the prevention, investigation and detection of crime. However, police forces must ensure that they fulfil their legal data protection and freedom of information obligations in relation to individual rights.***"

2.1.3. This suggests that prejudicing police work is acceptable, without offering guidance how it should be dealt with in practice. What is the Code recommending here?

2.1.4. The same is true for 4.32 in Principle 5 Accessibility which conflates three separate issues including different lawful obligations for ROPA and access limitation, in the same bullet point. *"Access to information must only be allowed to authorised individuals who need access for their lawful function. A force should ensure that it knows what information assets it holds. These assets should be stored in a way that ensures their efficient retrieval."*

2.1.5. It may be more effective to write the Code for staff seen from the Forces practical perspective as data users and with case studies after all of the Principles including accountability, under headings such as but not only, Purpose, Collection, Creation, Data types and reliability (Personal data, Fact vs Allegation / Opinion / Inference, Special category data, biometric data), Linking policing data with multiple data sources, Evaluating and actioning (including guidance on the use of data processing technology, information sharing and data processing by third-party services, prediction and data analytics, discrimination and bias in data including historic datasets), Records management (including taxonomy and meta data and ISO standards), Reviewing, retaining and disposing, Rights (to data subjects) and Responsibilities (Forces and third parties), Sensitive sources, and Audit.

2.2. Taxonomy cannot be optional in consistent national standards

2.2.1. A stated objective of *The Code of Practice for Policing information and records management* is to set national standards for police record keeping, to ensure consistency across forces, there must first be an understanding of what data is and that there is no such thing as a fixed data asset to "own", because the properties of personal data change over time and are better described as "controlled". While recognising a data life-cycle in Principle 3, "*Forces must maintain information and*

[12] See the ICO Guide to data processing for Law Enforcement | The right to rectification https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-rectification/

records throughout their lifecycle, to ensure their ongoing accuracy, reliability, integrity and usability, and to make sure that subsequent value is not compromised," the Code fails to give an understanding of what data is personal data, and which laws apply when to those different data types and their characteristics, in order to give users the confidence and authority needed to process lawfully and ethically, with consistency.

2.2.2. While mentioning meta data in section 4. Key Principles and in the consultation document 3.2, there is no reference to requirements for consistent universal taxonomy or orthography standards beyond the Plan. This is problematic for data accuracy and consistency, including reporting and auditing purposes if, *"The service should* ***strive*** *to develop and apply a consistent classification scheme or taxonomy, such as the Police Service File Plan,"* but not be required to all use the same one.

2.3. How might forces reconsider their role in personal data and policing records

2.3.1. The Consultation document speaks in section 3.8 and 3.11 of only two types of data (that may be sub-categories of personal data) in records created by police forces that are broadly organisational and administrative records (also referred to as corporate), and Police records, which contain information processed for a policing purpose.

2.3.2. It suggests that the core principles for processing all types of information that become a record are the same for the two categories, but does not match these with terms used in data protection law.

2.3.3. This fails to take into account personal data subsets of policing data that must be identified in order for forces to understand their different attributes and therefore lawful obligations. Namely differences between factual data (such as personal details, name, address, DOB), and inferred (allegations, assumptions, opinions, and inference that must be clearly identified, and where appropriate whose opinion it is) or data from the deceased, or special category (sensitive) data.

2.3.4. While both the new and the 2005 MOPI Code (4.3.2) includes an acknowledgement regarding, "*assessment of the reliability of the source*," it is given too little weight.

2.3.5. The new Code also fails to concretely address the implications of

(i) the *necessity* principle or explain what *necessary* means in data protection terms beyond the lay understanding of the word; or

(ii) the data minimisation principle, that data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

(iii) The Code makes no discernible attempt to explain the practical implications for police as duty bearers towards the people the data are about.

2.3.6. The nature of data is necessary to understand thoroughly because the obligations in law change over time, for example on the state the data may be retained in, whether identifiable, when it must be made anonymous, or deleted, or when the data subject must be informed about data processing this is not dependent on the type of record, but on the nature of the personal data held within it.

2.3.7. If a Force is expected to produce a guide for those people (data subjects) whose data it processes, it is hard to see that this Code gives enough information to help Forces understand data subjects rights and explain the necessary information for example what routine minimum information must be given to people in which circumstance. If those are not to be set out here, then the Code must at least indicate where they are set out.

2.4. Data subjects as rights holders and implications for duty bearers

2.4.1. When it comes to children in data records, Forces Records Management guidance, reviewed by defenddigitalme, tends to refer to children only from the perspective of police responsibilities in an investigation. Soham murders, missing persons, CSAM and indecent images, abuse investigations, or vetting those that wish to work with children in the disclosure and barring service. There is rarely mention of a child that would encourage police officers to see the child as a rights' holder. Under the UN Convention on the Rights of the Child, (UNCRC) children up to 18 years of age are considered rights holders and active participants in child rights realisation, who must be empowered to make claims and hold duty bearers to account for upholding children's rights. This absence of recognition of children as rights' holders means that there is also a corresponding absence of explanation of the role of police as duty bearers towards the child. We have not seen any Records Management "score, scan or scrap" decision flow charts that show at what point in a process a person who is described in the data, the data subject, should be informed of the processing or how they should be made aware of their rights such as to subject access, to accuracy, to correction, objection to processing, on profiling and automated decision making or routes for redress. This absence in guidance to respect the rights of the data subject, is reflected in the absence of these duties carried out in practice, and the impact of this is seen in the six areas of data processing failures we identify at the start of this submission.

2.4.2. There is no guidance on the role of parents and carers' in children's data processing and what Forces responsibilities are in practice towards the child or their responsible adult when processing data from a child, for example in a stop and search.There is no cross referencing to other Codes for example, or guidance to explain how this Code fits into the data processing elements of other Codes.[13]

2.4.3. There is no guidance on the rights of children when police are not asking them but others for use of children's data, and for example explaining that third parties cannot consent on behalf of children at scale i.e. a school so another lawful basis for data processing needs to apply.

Case study: an educational setting was responsible for the care of a sixteen year old, who was the victim of a crime. A police officer requested unrestricted access to the school pupil record, "*to see if they could find a reason why the pupil would have had anything to do with what happened.*" The Data Compliance Officer was concerned, knowing the pupil's record contained nothing of relevance to the incident, and that there was no grounds for a search of the record, but she considered it likely to prejudice the police based on her character records. It was "*a fishing expedition*", she said, yet the police were insistent. On asking for further information and raising an objection, the school Data Compliance Officer (DCO) was

[13] PACE Codes E and F 2018 have little guidance on data other than to say they need to respect data protection law -- but how does this code operate in conjunction on audio recordings for example https://www.app.college.police.uk/app-content/stop-and-search/

threatened with being taken to court by the officer. The DCO told us, "*it was ironic, I was being threatened with the law, but if I did give the police officer what I felt was unnecessary (as data controller for the school), it could result in me breaking the law*."

3. Question 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?

3.1. The Code must also address any requirements to understand the capability and standards in other organisations with which data may be shared or jointly created or processed, because the police forces reading this Code may think their data obligations finish at the end of their own direct processing of data that they "own", unaware that their legal duties extend to joint-controllership or processors' activity.

3.2. In terms of organisational capability, 5.1 suggests that, "*To ensure standards of competence, chief officers should also arrange the selection, training and professional development of those to be appointed to such posts.*"This is welcome but what does that mean in practice? "*All staff should understand their individual responsibility for how they process and handle information*," is an important concept and should be expanded upon. If a Chief Officer is to use this guidance in practice, how will it help them know what is the necessary standard of competence? Appointing a Data Protection Officer with no knowledge of policing may be obviously challenging to ensure an appropriate hire. Less obvious may be the Data Protection Officer who approaches all processing as questions of data protection alone and not social justice, who may not solve systemic problems, such as misuse of deceased children's personal data.[14] Data Protection Officers may not by default have skills in carrying out Equality Impact Assessments, Child Rights Impact Assessments[15], or understanding law that affects policing beyond routine data processing.

3.3. The importance and legal weight of the DPO role and views should be emphasised. Can DPOs veto policing decisions such as our six case studies? If views conflict, how are decisions recorded to reflect this, for accountability and audit purposes?

4. Question 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?

4.1. The key principles are selective and miss out for example, Accountability. How accountability is assigned is a significant change compared to older Data Protection law. Part 3, Chapter 2 of the UK Data Protection Act requires police to demonstrate that they comply with the principles and states explicitly that this is the responsibility of a data controller, as well as processor obligations, new under the GDPR.

4.2. Principle 3: Quality

On audit in 4.17, *Force systems and processes should provide an audit of who created a record, when and for what purpose.* There is no mention of auditability of any data extraction from records, its distribution and onwards use. This should be included, and

[14] The Guardian (2020) Met faces legal action over spies' use of dead children's identities https://www.theguardian.com/uk-news/2020/dec/07/met-police-legal-action-spies-use-dead-childrens-identities

[15] Livingstone, S. and Pothong, K. (2021) Child Rights Impact Assessment | A tool to realise children's rights in the digital environment https://digitalfuturescommission.org.uk/blog/what-if-childrens-rights-were-anticipated-at-the-very-start-of-digital-innovation/

require that a register is kept of any data extraction and distribution, including third parties, such as the Department for Education (DfE) approved external data shares.[16]

4.2.1. 4.19 Should expand upon the phrase, *"For records containing personal information, these data quality principles are set out in Part 3, chapter 2, section 37-39 of the DPA 2018 and article 5(c), (d) and (e) of the GDPR"* and set out what that means for data minimisation, data accuracy and storage limitation as well as including 5(f) on 'integrity and confidentiality'.It is unlikely they will be found and read, if not made explicit here.

4.2.2. It should also be emphasised that the use of he term 'principles' here is not a vague lay understanding of the word, but the data protection definition in law, and failure to comply with any of the data protection principles is extremely serious and may result, in the event of enforcement action, in receiving enforcement penalties of the higher maximum amount.[17]

4.3. Principle 4 Compliance

4.3.1. 4.22 Perhaps use the word disposal, not disposition. "Disposition can be either transferred to an archive or appropriate secure destruction."

4.3.2. Consider that in 4.22 obligations remain for the transferring organisation (likely as joint data controllers) in the event of data transfer, not only obligations on the data recipient.

4.3.3. The choice of heading here may also suggest that the other principles are only optional, if they do not come under the "compliance" heading, and yet those under retention, transparency, and quality are also matters for compliance.

4.4. Principle 5 Accessibility

4.4.1. 4.33 May wish to consider further themes under the guidance on accessibility a) unauthorised access in the event of security breaches that result in data being withheld (ransomware attacks)[18] which is more practical "what should forces do" beyond 4.28 and 4.29 that there should be suitable security requirements and b) in the event of system failure (preventing data access) and c) accessibility-by-design in terms of inclusion i.e. due to colour blindness or dyslexia within the force as well as external access to appropriate data in terms of the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018[19], rather than only as described in the context of business continuity as a result of data loss.

4.5. Principle 6: Review and Retention

4.5.1. Legacy migration

It may be incorrect to suggest that, "*Records that need to be preserved for future use should be migrated to newer formats and/or systems when the current ones become obsolete. To ensure that the context is not altered or lost, the migration should include all relevant metadata."* It can be very expensive and time intensive to carry out legacy data migrations, which are often problematic due to incompatible meta data structures, design and creation of organisational structures' start dates in new systems, or missing

[16] Department for Education (DfE) approved data shares with external, third-party organisations. We would recommend a different technical design however better than multiple separate spreadsheets over time, that should be searchable and consistent in organisational taxonomy and spelling. https://www.gov.uk/government/publications/dfe-external-data-shares

[17] The Information Commissioner can issue a monetary penalty for failing to comply with Part 3 of the Act. In practice, the higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/

[18] ICO Guidance for law enforcement on data breaches Personal data breaches https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/

[19] Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps

fields. It may be more appropriate to state that where data is necessary to be retrieved or for reference, it may or may not be appropriate to keep it in an accessible but archived system. Only the minimum necessary viable data should generally be migrated into new systems.

4.5.2. Consistency across forces and decisions is easy on the easy things

4.5.2.1. In 4.36 there is no guidance given when it comes to making the difficult decisions and the Code will fall down on trying to deliver consistency and high standards, if this is not set out. Guidance is rarely needed on easy things, but it is the difficult things that need addressed. "*Where a decision is made to retain a record for longer than the designated retention period, the justification for the extended timescale must be recorded."* This is very weak and needs thorough guidance if outliers are to be made in a consistent way.

4.5.2.2. We have reviewed a number of Forces' Retention Schedules published online. On retention it appears current practice commonly has three common flaws and these are not picked up in the Principles of the Code.

1. **Rather than assessment of retention according to the targeted necessity and proportionality of the personal data within the records, it is common for retention schedules, to assign blanket retention periods (*Minimum retention, and MOPI grading (if applicable*)) by the content or activity type of the record, not the nature of data in each part of the record which may have different legal obligations such as biometric data, religion, ethnicity or be opinion vs fact.**

   i.e *Bail cards, MoPI 3 (minimum of 6 years + clear),* or *Collisions Minimum of 6 Years or until the injured party is 21 years old whichever is the longest. Fingerprints and palm prints, For adults is retained indefinitely where there is a conviction, retained for 3 years where there was a charge but no conviction (and no previous convictions recorded) and deleted immediately if not charged (a single search is permitted before destruction).* ***For under 18s is retained indefinitely."*** *(We question for example, is this correct for u18s, as it appears excessive retention.)*

   "The main characteristic of MoPI groupings is that they help determine how long individual and linked records (e.g. registered crime files) need to be kept."
   (MPS RM policy, compliance and guidance v1.0 2017)[20]

   In our opinion, a review could assess whether MOPI group gradings are contributing to the difficulty in understanding the nature of personal data and the applicable obligations towards personal data within records, and the separation between victims and perpetrator of crimes, given that the gradings do not distinguish between them.

2. **As regards archiving, Guidance should be able to offer decision makers in today's practice with a clear and consistent lawful basis for standard practice. Today's policies often appear based on opinion which may be inconsistent.**

   For example in Sussex and Surrey's retention schedule[21] there is unclear lawful

[20] Met Police Service Records Management policy, compliance and guidance v1.0 2017 https://defenddigitalme.org/wp-content/uploads/2021/03/strategy-governance-mps-records-management-policy-compliance-guidance.pdf

[21] Surrey Police and Sussex Police Retention and Disposal Schedules Introduction and Guidance (2019) https://defenddigitalme.org/wp-content/uploads/2021/03/retention_schedule_may_2019-Sussex-and-Surrey.xls

basis for what appears a relatively arbitrary process of decision making based on opinion, and a distinction made between volume data and that of celebrities.

"Under the Surrey and Sussex Police Retention Schedule some records are kept for historical reasons. For retention scheduling purposes historical is defined as a record that has historical value to Surrey and Sussex Police, the people of Surrey and Sussex and future generations wherever they come from. Historical value is determined by the context and the narrative of the record concern and how it will assist future historians in writing the history of Surrey and Sussex Police, the county of the Surrey and Sussex and the Police Service nationally or internationally."

"It is anticipated that majority of records kept for historical reasons will concern the organisation and personnel of the Surrey and Sussex Police. Some records concerned with the investigation of crime will only be kept if they are considered 'infamous' or of sufficient public awareness to have made the local and national media. Volume Crimes are unlikely to feature unless they have involved persons of national interest, for instance Celebrities."

3. **The concept that Information records are corporate property to be owned as read in many forces' records management compliance guides, such as the Met Police 2017 Guide (due for review in 2021). This can often conflict even within the same guidance.**

   This understanding may benefit from being understood instead as a process along a timeline of multi-way different parties and the roles and responsibilities around the control of data, involving processing and rights of the data subjects, rather than thinking of data as an owned asset that belongs to a single force and seeing the responsibilities around data only as something static that police are involved in only at the point of direct use by a human police officer.

4.6. Principle 7 Disposition

4.6.1. It may be important not to inadvertently suggest that using a delete button is generally the same or sufficient for data destruction from records. *"4.41 Where physical destruction is not possible – for example, where an IT system does not have a delete functionality".*

4.6.2. Is disposition really the correct term to use here?

5. Question 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?

5.1. It is welcome that paragraph 6.7 includes, "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 is clear.

5.2. Data sharing registers

5.2.1. The Code is missing any guidance on the requirement to maintain a log[22] or register of data distribution / "data sharing" and data copying as part of a record of processing

[22] The ICO (Guide for Law Enforcement) Logging | It is important to monitor and audit internal processing within any automated processing systems you use, and to know which third parties you have shared data with https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/logging/

activities under Article 30 of the GDPR[23] and the UK Data Protection Act 2018 Part 3, Chapter 4, Section 62, "Logging".[24]

5.2.2. In the same way that 4.46 mentions the requirement, *"Forces should keep a catalogue of records that have been permanently archived, including detail relating to the nature of the record, their context and their location,"* the same express guidance should be given for all data sharing. It is a requirement to keep a register of all processing under ROPA, that *"You have an internal record of all processing activities carried out by any processors on behalf of your organisation"* including any domestics use and abroad, with reference to section 6.9/6.10 of the Code *"details of transfers to third countries, including a record of the transfer mechanism safeguards in place."*

5.3. Distribute access not data

5.3.1. 'Information Sharing' is an outdated concept in modern data management and one that should be discouraged. Forces should be encouraged not to "share data" by extracting data, making copies that are hard to keep accurate, ensure rights are met, or have oversight of, but to permit authorised access, using role based security, to original source data though appropriate systems such as APIs that can be audited. Distribute access, not the data.

5.3.2. A key problematic issue in data management, includes the loss of oversight of data once copied and shared and the ongoing lawful basis for processing in an onwards chain.

5.3.3. Whilst the Code says in paragraph 3.10 that some information recorded for policing purposes may be processed under Part 3 of the DPA 2018 and other information under part 2 DPA 2018 and the GDPR, it is not explained how this will work in practice and therefore is very unclear and suggests lack of clarity in the understanding of which lawful basis should apply when to what data processing.

5.3.4. Transfers of personal data in records needs a dedicated set of explanatory guidelines. If there is a general rule that personal data should not be extracted from systems, for sharing in email, printing, or distribution, there should be clear guidance for exceptions to this. If such extraction and transfer or distribution is routine, then the guidance should be clear on expected practice,what it means for the ongoing oversight by the data controller for the record of processing (ROPA), and its audit trail.

5.3.5. Guidance should remind Controllers of the required conditions for transfers abroad of personal data to persons other than relevant authorities, check that the transfer is covered by adequacy regulations and that the transferring controller must— (a) document any transfer to a recipient in a third country other than a relevant authority, and (b) inform the ICO about the transfer.

5.4. Data linkage

A further problematic issue in data management, is the joining up of existing data held, with data obtained from other sources, including sources not intended for policing that are repurposed for policing, creating new knowledge and without the awareness of the data subjects.

5.4.1. While there is a final paragraph on *Obligations of those receiving police information,* there is no guidance for example on the obligations on police receiving information from other third parties and data linkage together with policing data sources and retention of joined-up data, or the obligations for purpose limitation and fair processing. What lawful basis if any exists for joining up police information and school records for example, whether at school level or from the National Pupil Database? What are the public's

[23] The GDPR Article 30 Records of processing activities https://www.legislation.gov.uk/eur/2016/679/article/30
[24] DPA 2018 Part 3 Section 4 s62 "Logging" https://www.legislation.gov.uk/ukpga/2018/12/section/62/enacted

reasonable expectations of police access to all DVLA records? How do the police force understand the legal obligations upon them, created as a result of the nature of the external data i.e. the purpose for its collection, the legal basis used to obtain that dataset by the Data Controller, and what people were told at the time of collection? Who is accountable for communication to the data subjects?

6. Question 6. To what extent do you think that the Code sufficiently covers the relevant data protection safeguards?

6.1. These seem missing completely. There is nothing on how these are to be consistent or communicated. Although the word safeguards is mentioned in 3.11, 3.12, and 4.47 there is no indication of when what is needed or required in law. For example, there is no guidance about data used in not profiling children (GDPR Recital 71), prediction, or automated decision making (A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law)[25], key elements of data protection guidance and in particular with additional safeguards required for children and young people, recognised as vulnerable persons.

6.2. Therefore a supplemental section is needed on safeguards for specific types of data processing with guidance on what they should be, for example

1. safeguards for children's data processing (and other vulnerable persons),
2. for all data subject rights to be told of safeguards,
3. safeguards on compatibility of purposes,
4. safeguards on limitations of consent (that it must be affirmative and freely given without prejudice, and that consent may be invalid as a basis for data processing where there is an imbalance of power),
5. safeguards on automated decisions, (DPA 2018, Part 3, Chapter 3, s50)
6. safeguards on data about criminal convictions,
7. safeguards on data about vital interests,
8. safeguards on data about preventing fraud,
9. safeguards on data about legal claims and judicial acts,
10. safeguards on data for archiving purposes, and safeguards on data in international transfers to third countries and others.

6.3. *"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and **safeguards** concerned and their rights in relation to the processing of personal data."* (The GDPR Recital 38)

6.4. *"Natural persons should be made aware of risks, rules, **safeguards** and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*" (The GDPR Recital 39)

6.5. *"Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, **safeguards** should ensure that the data subject is aware of the fact that and the extent to which consent is given."* (The GDPR Recital 42)

6.6. *"In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into*

[25] Right not to be subject to automated decision-making **DPA 2018 Part 3, Chapter3, s49 and s50** safeguards https://www.legislation.gov.uk/ukpga/2018/12/section/49/enacted

account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and ***the existence of appropriate safeguards*** *in both the original and intended further processing operations.*" (The GDPR Recital 50)

6.7. *"The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her….****In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.****"* (The GDPR Recital 71)

6.8. *"This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data* ***including appropriate safeguards for the data subjects.*** *Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects."* (The GDPR Recital 102)

6.9. *"The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers* ***subject to appropriate safeguards***…" (The GDPR Recital 107)

6.10. "A transfer of personal data to a third country or an international organisation is **based on there being appropriate safeguards**" (DPA 2018, Part 3 Chapter 5 Section 75)

6.11. *"The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be* ***subject to appropriate safeguards for the rights and freedoms of the data subject****.*." (The GDPR Recital 156)

6.12. *"Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)...(e)* ***the existence of appropriate safeguards,*** *which may include encryption or pseudonymisation."* (The GDPR Article 6(4)(e))

6.13. *"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law* ***providing for appropriate safeguards for the rights and freedoms of data subjects.*** *Any comprehensive register of criminal convictions shall be kept only under the control of official authority."* (The GDPR Article 10)

6.14. *"Where personal data are transferred to a third country or to an international organisation,* ***the data subject shall have the right to be informed of the appropriate safeguards*** *pursuant to Article 46 relating to the transfer*." (The GDPR Article 15(2))

6.15. Where rights are restricted on the grounds of national security, public security, or 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; there must be "specific provisions" as regards *"(f) the storage periods and the **applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing**; and (d) **the safeguards to prevent abuse or unlawful access or transfer;***" (The GDPR Article 23)

6.16. There is no guidance given on when Forces may need to consult the supervisory authority (The ICO) prior to processing where a data protection impact assessment[26] under the GDPR Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. And that they are required to *"provide the supervisory authority with the measures and **safeguards provided to protect the rights and freedoms of data subjects**…"* (DPA 2018, Part 3, Chapter 4, s64 and s65)

6.17. **The Code is missing any guidance on appropriate safeguards as regards sensitive processing.** In the context of law enforcement, personal data will often be sensitive. When it is, Forces must be able to demonstrate that the processing is strictly necessary. It is not enough to argue that processing is necessary because they have chosen to operate activities in a particular way. The question is whether the processing is necessary for the stated purpose. Sensitive data as defined in section 35(8) as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

If forces are carrying out sensitive processing based on the consent of a data subject, or based on another specific condition in Schedule 8 of the Act, they must have an appropriate policy document in place, according to the ICO including any limitations of that consent.[27] This has implications to ensure that the infrastructure and mechanisms exist to make that happen and record such decisions. This should be added to the Code.

7. Question 7. To what extent do you think compliance with the Code will support public confidence in the way forces manage their information and records?

7.1. The introduction both bypasses one of the most important areas for public trust and accountability, and points to why this Code fails to deliver on these two points, namely on safeguards for covert operations. While the Code on 3.12 states, *Covert material contained within police records is bound by additional safeguards contained within the Investigatory Powers Act 2016, Regulation of Investigatory Powers Act 2000 and associated codes of practice.* There is no transparency for every day members of the police force or the public what this means, and it is complex to try and understand a

[26] The ICO | Data protection impact assessments https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-impact-assessments/

[27] Guide to data processing for law enforcement (sensitive data) purposes.https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/ and conditions for sensitive data processing https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing/

variety of different documents across different areas of practice. If indeed, as stated in 3.13, the goal is that "*The code and supporting national guidance should promote consistency across the service and should facilitate a unified approach to the identification and management of risk and vulnerability"* then it must not workaround the difficult things, because it becomes a meaningless nice-to-have without teeth or actual effective guidance for when it is most needed.

7.2. Police forces cannot expect engagement to rebuild public confidence as long as they fail to be honest and transparent about covert surveillance of victims and family members.[28]

7.3. The Code does not address the significant public concerns that exist of data collection from policing non-criminal activity.

7.4. And the Code does not address any issues around data bias and discrimination and what to do about it. 85% of Black people are not confident that they would be treated the same as a white person by the police.[29]

7.5. The Code falls short of what is needed to enhance public confidence, not because of what is in it on paper, but because of what is missing and its disconnect with applied practice.

8. Question 8. Do you have any comments on potential positive or negative impacts of the Code on individual members of the public?

8.1. There is no guidance on records about more than one person. This is very important in policing because the record about X may contain allegations from person Y or about a third party Z, or personal data that is personal and identifying even if not about an individual such a community e.g. Travellers on Site A. Guidance must include how to address rights if data is about multiple persons, ie. fairness, or subject access requests.

8.2. Such processing may have positive outcomes, for the purposes of developing strategies such as 'no cold calling zones' targeting those who commit distraction burglaries, whilst protecting potential victims, or repeat victim protection, but it may also be used with negative outcomes, such as the over profiling of black young men for stop-and-search.

8.3. There is also no guidance on the implications for building crime intelligence and data analysis of risks and trends through profiling behavioural interactions together with other public bodies data, with the NHS for example, by the Counter Fraud and Security Management Service (NHS Business Services Authority) or Drugs Intelligence work. There should be tough and transparent safeguards wherever the policing interactions are not foreseeable by members of the public including the use of public services.

9. Question 9. How easy or difficult do you think it will be to implement the Code across forces?

9.1. There are large gaps left open for interpretation. For example '*2.8 Chief officers must be cognisant of the legislation, codes and guidance that apply to their area of business',* will unlikely to be consistently applied, unless consistently made available to access in one place with links/ referenced from this Code. There is no guidance on the most challenging areas of data management and therefore it is not intentional about consistent good practice.

[28] Deighton Pierce Glynn | Brooks/Lawrence Spy named by UnderCover Police Inquiry (UCPI) https://dpglaw.co.uk/brooks-lawrence-spy-named-undercover-police-inquiry-ucpi/

[29] Clearview research (2020) Failures to secure black people's human rights enquiry | The Joint Committee on Human Rights https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/559/55906.htm

10. Question 10. Do you have any suggestions that you think would help the implementation of the Code?

10.1. Encourage forces to collect less data. Data minimisation principles are not about looking retroactively at mass data programmes to shave off and weed out data systems, but to understand at the root of any process, "*personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*."[30]

10.2. Process diagrams could be used to demonstrate when certain common actions should happen, and where the role and responsibility may rest that the Code seeks to improve, mapping where the activities happen such as telling people how their data are used, or decision making on record weeding and destruction, mapping the responsibility the make it happen onto the roles across each model process.

11. Question 11. Do you have any other comments on the draft Code?

11.1. Other related legislation

To answer the question, "*How does the Code fit with other information management legislation*?" a list is given of other Codes and legislation but because it is stated as "all relevant legislation and other codes" it might suggest this is exhaustive. But it is not, noticeably leaving out for example, the Convention 108 or the Equality Act 2010 (despite a mention in the draft Code 4.8). The list should either be made inclusive to be adequate to meet the stated goals of the Code information and audit purposes, or state it is non exhaustive and where the complete list should be found. Chief Officers cannot guess what they do not know that they don't get told, and they cannot be expected to use or be held accountable in an audit against the Code, for information that they have not been given.

11.2. The Common Law Duty of Confidentiality and records of deceased persons

There is no guidance as a result of the incomplete list, on how to treat the personal data of the deceased, since the GDPR for example, only applies to living natural persons, and while relatives may be affected by data processed about a deceased person this may not be immediately clear to Forces that data processing laws and other law must still be considered. A common law duty of confidentiality and ethical practice are expected to apply to the deceased, requiring that confidentiality obligations continue to apply after death.[31]

Contact

Jen Persson Director, defenddigitalme
March 2021

[30] Recital 39 The GDPR
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

[31] The Common Law Duty of Confidentiality was applied for example to deceased patients' records, as per the Information Tribunal Appeal Number: EA/2006/0010 of 17 Sep 2007# between Pauline Bluck, the Information Commissioner and Epsom & St Helier University NHS Trust and Lewis v Secretary of State for Health [2008] EWHC 2196. In the case of Z v Finland (1997) 25 EHRR 371 the European Court of Human Rights found that the importance of confidentiality in medical data went beyond protection of the individual, but to the protection of the medical system to preserve public confidence in health services, in particular to ensure that those in need of assistance are not deterred from sharing information that they need to with health services and receive appropriate treatment, to ensure the promotion of the collective good of public health systems, such as participation in public health vaccination programmes.