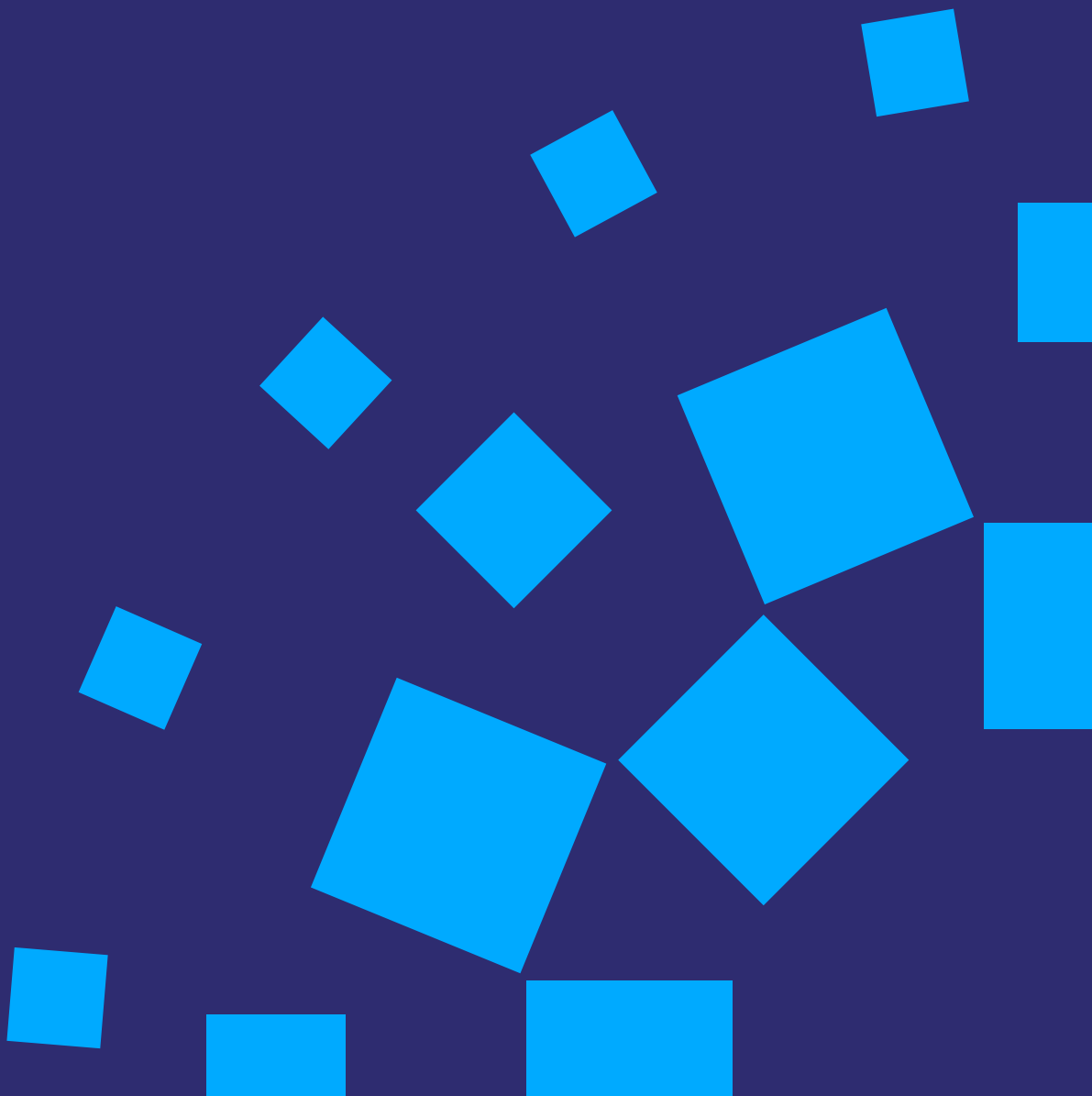
College of Policing

Working together to keep people safe

Police Information and Records Management Code of Practice

Consultation



College of Policing Limited
Leamington Road
Ryton-on-Dunsmore
Coventry
CV8 3EN

For any other enquiries about the content of the document, please email **contactus@college.pnn.police.uk**

Contents

1 Statutory basis of the Code

1.1 This Code of Practice comes into effect on XXXXXXXX.

1.2 Nothing in this Code alters the existing legal powers or responsibilities of any police and crime commissioner (PCC) or equivalent, chief officer of police, or other person.

1.3 The College of Policing has issued the Police Information and Records Management Code of Practice ('the Code') as a code of practice under section 39A of the Police Act 1996.

1.4 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)
- relates specifically to chief officers in the discharge of their functions

2 Purpose of the Code

2.1 The Code replaces the Management of Police Information (MoPI) Code of Practice 2005.

2.2 The purpose of this Code is to set national principles for police information and records management, and to provide a template against which records management audits can be based. It provides a framework to support a cohesive, ethical, effective and lawful approach to the management of information and records within the police service. This, in turn, will maximise the opportunities and benefits that good information and records management provides, thereby improving accountability and increasing the public's confidence in the way that their information is managed.

2.3 The Code broadens the applicability of the original MoPI beyond records that contain police information, to include police corporate governance records, and it updates the Code in light of related legislative – and other – developments. The Code also introduces archiving in the public interest into the police records management regime.

2.4 The Code is available for adoption by other agencies, including other police forces not covered by section 1 of the Police Act 1996, PCCs or equivalents, and law enforcement agencies within the UK that exchange information with the police service in England and Wales.

2.5 The processing of information and records management in the service is subject to a number of statutory obligations and standards. This Code is not exclusive and must be considered in conjunction with all relevant legislative and regulatory requirements, including the General Data Protection Regulation (GDPR), Data Protection Act (DPA) 2018, Human Rights Act 1998, Criminal Procedure and Investigations Act 1996, Protection of Freedoms Act 2012, Investigatory Powers Act 2016, Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004.

2.6 The Code should also be considered in conjunction with existing and future codes of practice, including (but not limited to):

- the Police National Computer (PNC)
- the Police National Database (PND)

- the Law Enforcement Data Service (LEDS)
- other codes, such as:
  - the Code of Practice on the management of records issued under section 46 of the FOIA
  - the Information Commissioner's Office (ICO) Code of Practice on data sharing

The Code must also be applied alongside other legal and policing duties and responsibilities, such as those set out in the College of Policing Code of Ethics.

2.7 National guidance will advise police forces on how this Code should be implemented to ensure compliance with the aforementioned legislative framework.

2.8 Chief officers must be cognisant of the legislation, codes and guidance that apply to their area of business.

Role of other agencies

2.9 Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) monitors and reports on the efficiency and effectiveness of the police, with the aim of encouraging improvement.

2.10 The ICO is the independent regulatory authority responsible for upholding information rights in the UK, most prominently the GDPR, the DPA 2018 and the FOIA, under which it has powers to respond to concerns from data subjects and to take action to ensure that organisations meet their information rights obligations.

2.11 The College of Policing published the Code and is responsible for ensuring that it remains accurate and relevant for policing. The College will also publish supporting guidance referred to throughout this Code.

2.12 The National Police Chiefs' Council (NPCC) Professional Portfolios will oversee police records and information management nationally, publishing policy and procedures as necessary.

2.13 PCCs, and equivalents, have a duty to hold chief constables to account for all their functions. This includes responsibility for ensuring force compliance with this Code.

3 Introduction

3.1 Information is a key asset to the police service. The effective management of information throughout its lifecycle (creation, use, retention, appraisal and disposition), and across all aspects of policing, is vital to delivering the core priorities of the service: to protect the public and reduce crime.

3.2 Information must be recorded and records must be created when it is necessary for a policing purpose or for organisational business. Forces should capture sufficient technical and contextual information (metadata) to be able to handle and control force information, to determine access, and to manage, find and understand that information in the future. Metadata should be kept in such a way that it remains reliable and accessible for as long as it is required.

3.3 The recording of police information must adhere to the separate guidelines that support this Code.

3.4 To carry out the functions of policing, the service has to process personal and organisational information from a range of sources and in a number of different forms.

3.5 ISO 15489-1:2016 defines a record as 'information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business'.

3.6 References to records may refer to any particular format or media, including:

- records containing biometric information
- hardcopy records, including (but not limited to):
  - paper
  - microfilm
  - microfiche
  - DVDs
  - audio and video tapes

- digital records, including (but not limited to):
  - databases
  - information created on mobile devices
  - spreadsheets
  - word-processed documents
  - email

3.7 Due to the nature of policing, it is essential to distinguish between information processed for a policing purpose and information required for business functions that support the service to deliver.

3.8 Records created by police forces broadly fall into two categories.

- Organisational and administrative records (also referred to as corporate), which contain information processed to enable the discharge of police services, such as financial information, policies and procedures, and information relating to employees.
- Police records, which contain information processed for a policing purpose, namely:
  - protecting life and property
  - preserving order
  - preventing the commission of offences
  - bringing offenders to justice
  - any police duty or responsibility arising from common or statute law

3.9 It should be noted that the policing purpose definition is wider than the following definition of law enforcement purpose, which is given in Part 3 of the DPA 2018:

> '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.'

3.10 Consequently, some information recorded for a policing purpose may be processed under Part 3 of the DPA 2018, while other information may be processed under Part 2 of the DPA 2018 and the GDPR.

3.11 The core principles for processing all types of information that become a record are the same for the two categories. However, the nature of information recorded for a policing purpose requires extra safeguards, which are reflected in this code and supporting national guidance.

3.12 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.

3.13 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.

4 Key principles governing the management of police records and information

4.1 Creating and managing information according to the principles in this Code will result in information that:

- can be located, accessed, retrieved and accurately interpreted when needed
- can support effective decision making, forecasting and efficiencies
- can be trusted as complete and accurate, increasing public and employee confidence
- has been legally and ethically collected, and is used for the intended purpose
- is kept for an appropriate time period, to ensure that it is retained for no longer than is required for the purpose for which it is being processed

4.2 The value of information is often overlooked. Poor management of information can result in:

- an impact on individual rights and entitlements causing personal distress
- lost opportunities for information sharing
- poor decision making
- inconsistency of approach to the management of risk and vulnerability across the service
- reputational damage
- unnecessary costs and inefficiencies, such as regulatory fines, time to retrieve information, and the storage and preservation of redundant information
- inability to understand the level of risk that a person may present, or the level of risk that a person may be subjected to

4.3 Good information and records management mitigates information-related risks and creates opportunities.

Principle 1: Governance

4.4 Police forces must have appropriate governance arrangements for information and records management, including accountability and ownership. The chief constable, as data controller, is responsible for ensuring that appropriate technical and organisational measures are in place to comply with this Code, and that these measures are updated and reviewed when necessary.

4.5 Forces should designate officers or staff of suitable seniority and knowledge as senior information risk owners (SIROs), information asset owners (IAOs) and data protection officers (DPOs). Force governance should incorporate information risk and include clear routes for escalation.

4.6 Forces must have roles in place that are responsible for records management, information security, data protection and freedom of information on a day-to-day basis.

4.7 Chief constables should promote an environment and culture whereby both the benefits and the responsibility of holding the public's information are understood, ensuring that access and retention is legitimate.

4.8 Forces must ensure that they have the documentation required by data protection legislation and the Equality Act 2010 in place. This includes:

- data protection impact assessments (DPIAs), when processing is likely to result in a high risk to individuals' rights and freedoms
- equality impact assessments (EIAs) and appropriate policy documents, where required, when processing sensitive personal data

4.9 The service should strive to develop and apply a consistent classification scheme or taxonomy, such as the Police Service File Plan.

4.10 Records created and acquired during the performance of duty, and any duplicates of these records, remain the property of the force. Forces should have systems and processes in place to ensure that these records are accounted for when individuals leave the organisation.

4.11 Chief officers will establish and maintain information management

policies within their forces that comply with national guidance and standards to be issued under this Code, unless that guidance is superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996.

4.12 Strategies and tactical plans should be developed to embed good practice and to encourage a culture where good information management is seen as part of everyone's role.

Principle 2: Transparency

4.13 Forces must be appropriately transparent with the public about the nature and type of the records and information that they hold. Records are required to stand up to scrutiny and to meet legislative and regulatory requirements, including individual rights and entitlements. 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. Part 3 does not specifically refer to transparency in terms of the processing of personal data, as 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.

Principle 3: Quality

4.16 Forces must maintain information and records throughout their lifecycle, to ensure their ongoing accuracy, reliability, integrity and usability, and to make sure that subsequent value is not compromised.

4.17 Force systems and processes should provide an audit of who created a record, when and for what purpose. There should also be a record of each occasion when the record has been accessed, stating when it was accessed, by whom and for what purpose. If the record has been changed, either by an individual or due to a system upgrade

or migration, it should be recorded by whom or how the record was changed, for what reason and the nature of the changes. Forces must have data quality audit and compliance arrangements in place.

4.18 All police information must conform to the data protection principle of accuracy, ensuring that it is correct, up to date, relevant, complete and not unnecessarily duplicated. Forces should comply with appropriate published national recording standards.

4.19 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 .

Principle 4: Compliance

4.20 Forces must put arrangements in place to ensure that information is handled in line with relevant legislative and regulatory obligations, including the supporting national guidance.

4.21 Policing information must undergo evaluation appropriate to the policing purpose for which it was collected and recorded. All police information should be evaluated to determine:

- threat, risk, harm and/or vulnerability
- provenance
- quality (including conformity, completeness, duplication and accuracy)
- continuing relevance to a policing purpose
- what action, if any, should be taken

4.22 IAOs must be aware of their obligations to manage information and the metadata appropriately, including retention, disclosure, preservation and disposition. Disposition can be either transfer to an archive or appropriate secure destruction.

4.23 Personal data must not be excessive and must be relevant to the purpose for which it was collected.

4.24 The standards within this Code and national guidelines should be built into the design, development, procurement and functionality of IT

systems and applications, as well as any changes to existing systems.

4.25 A 'privacy and security by design and default' approach should be built into change projects and new IT requirements. The opportunity to implement automation of review, retention and disposition processes should also be considered.

4.26 The scope of any asset, and the criteria against which personal data will be collected onto it, must be clear and defined to avoid any ambiguity or ad-hoc recording.

4.27 Where possible, the existence of the asset should be publicly known, along with the criteria above. The information should be searchable and accessible to enable individuals to exercise their data protection rights, such as appropriate access.

4.28 Information and metadata must be suitably secured and stored, managed, handled, maintained and disposed of in accordance with the Government Security Classification Scheme.

4.29 Forces should issue guidance, in line with the Code and national guidance, detailing the policies, procedures and control measures that should be in place to protect information assets and personal data from:

- unauthorised or accidental access
- amendment of, or loss of, information in line with data protection security requirements

4.30 Forces should be able to demonstrate that their information and records management practices comply with the standards detailed in this Code and their force policies. Forces should develop plans to address shortfalls and pursue continuous improvement.

Principle 5: Accessibility

4.31 Force systems used to manage information and records must have the functionality necessary for adherence to the principles in this code.

4.32 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.

4.33 Business continuity arrangements must be in place to ensure that any loss of information is appropriately managed, and that control measures are in place to minimise risk and disruption to day-to-day business.

Principle 6: Review and retention

4.34 Forces should implement the appropriate review and retention procedures and periods in line with national guidance – including College information and records management guidance, guidance relating to specific material (such as covert, biometric and evidential material), and any retention schedule published by the NPCC – in order to:

- protect the public and help manage the risks posed by known offenders and other potentially dangerous individuals
- ensure compliance with the relevant legislation

4.35 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.

4.36 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.

4.37 Forces should put arrangements in place for the selection of records for permanent preservation, as well as records subject to ongoing public inquiries, in line with published guidance.

4.38 Under the Inquiries Act 2005, forces have an obligation to preserve relevant records for the inquiry for as long as necessary. The obligation to retain documents will remain throughout the duration of the inquiry.

4.39 Police records must only be retained for as long as there is a legitimate organisational or policing purpose, while being cognisant of records where wider public interest, statistical, scientific or historical purposes may necessitate extended or permanent retention.

Principle 7: Disposition

4.40 When information and records are no longer required, or have reached the end of their designated retention period, arrangements must be in place to ensure that appropriate methods are used for their disposition, which may include secure destruction.

4.41 Where physical destruction is not possible – for example, where an IT system does not have a delete functionality – methods of minimising the risk to further use or exposure must be considered (ie, putting beyond use or restricting access).

4.42 Forces should have arrangements in place to archive selected documents for permanent preservation, in line with national guidance, where they are no longer required for an organisational or policing purpose. This may be in partnership with an external archive service.

4.43 Archived physical records, such as paper and microfiche, should comply with the relevant care and conservation British Standards detailed in national guidance.

4.44 In the case of digital records that are intended to be archived, care must be taken to ensure long-term accessibility, integrity, usability, reliability and authenticity in the case of format obsolescence, including minimising the loss of quality, data or metadata.

4.45 Forces that choose to archive records for permanent preservation with an external provider should agree governance arrangements through an information-sharing agreement. This agreement should identify the data controller, clarify who is responsible for freedom of information and data protection obligations, and outline a process for recalling records.

4.46 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.

4.47 Forces should have:

- appropriate arrangements to keep collections, in all formats, safe and accessible
- resource commitments – such as people, facilities, finance and IT – necessary to maintain the arrangements
- coherent policies, plans and procedures
- an appraisal, selection and sensitivity review process
- arrangements that build in data protection legislation safeguards
- a disaster recovery plan

5 Organisational requirements

Personnel capability

5.1 Chief officers should identify the key posts required for the management of police records, and should ensure that the posts are filled and that the function is suitably resourced. To ensure standards of competence, chief officers should also arrange the selection, training and professional development of those to be appointed to such posts.

5.2 All officers and staff employed by forces will be involved in creating records and processing information. Consequently, chief officers should ensure that they are given the necessary training and ongoing development consistent with their role. All staff should understand their individual responsibility for how they process and handle information.

5.3 Training for managing records and information management is not only to ensure compliance with this Code and the legal framework, but also to ensure the consistency of procedures throughout the police service.

Organisational capability

5.4 Chief officers should ensure that staff have the appropriate equipment, accommodation and systems to comply with this Code.

5.5 Chief officers should also ensure that their force has the tools and systems to manage and organise information throughout its life, including backup systems to recover from systems failure.

6 Information sharing

6.1 Forces should comply with the ICO Code of Practice on data sharing when sharing personal information. Information sharing by forces for specific law enforcement purposes is subject to Part 3 of the DPA 2018, which provides a separate but complementary framework from the general processing provisions under the GDPR and Part 2 of the DPA 2018.

6.2 The GDPR and data protection legislation provides a framework to ensure fair, lawful and proportionate data sharing, and should not be perceived as a barrier to appropriate information sharing. Information sharing is beneficial for society as a whole, and sometimes it can be more harmful not to share information.

Sharing of policing information within the UK police service

6.3 Information recorded for police purposes, as well as any assessments of its reliability, should be made available to any other police force in England and Wales that requires the information for policing purposes. However, this is subject to any constraints arising from guidance based on section 6.16 below. Sharing this information must be lawful, proportionate and reasonable.

6.4 Other police forces in the UK should be afforded the same degree of access to information that has been recorded for police purposes by police forces in England and Wales. However, this is subject to the same constraints outlined in the previous paragraph. The chief officer responsible for the record must also be satisfied that the police force seeking access to the information applies the principles set out in this Code.

6.5 Chief officers may arrange for the sharing of information with other police forces in the UK, in accordance with the two preceding paragraphs, to be carried out by:

- response to bilateral or multilateral requests for information to police forces
- holding such information on IT systems to which the police forces referred to above may be given direct access

- the timely uploading of quality data to national systems

Sharing of policing information with UK-based non–law enforcement agencies

6.6 Chief officers will continue to comply with any statutory obligations to share information with bodies other than police forces in England and Wales.

6.7 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.

6.8 Personal data processed by police forces for law enforcement purposes under Part 3 of the DPA 2018 may be shared outside the police force, for non–law enforcement processing under the GDPR, provided that the processing is authorised by law.

Sharing policing information outside the UK

6.9 Chief officers may arrange for law enforcement authorities outside the UK to receive police information where the chief officer is satisfied that it is reasonable and lawful to do so for a policing purpose. In deciding what is reasonable, chief officers should have regard to any national guidance or code, as well as considering any protocol – whether at national or local level – that may be agreed with people or bodies needing to receive such information.

6.10 Where a request is made to transfer personal data to forces outside the UK for a law enforcement purpose, chief officers must apply the criteria contained within sections 72-78 of the DPA 2018 before agreeing such a request.

Protection of sensitive police information and sources

6.11 National guidance may provide for special procedures to be applied to a request for access to information recorded for police purposes, in cases where it is necessary to protect the source of sensitive information or the procedures used to obtain it.

Obligations of those receiving police information

6.12 In making national or local agreements and protocols for the sharing of police information with people or bodies other than police forces, or in responding to individual requests for information outside such agreements or protocols, chief officers must require that those to whom information is made available comply with the following obligations.

- Police information made available in response to such a request should be used only for the purpose for which the request was made.
- If a person or body who requests police information also has access to other information – at the time or later – that suggests the requested information is inaccurate or incomplete, the person or body should inform the relevant chief officer of this inaccuracy or incompleteness at the earliest possible moment. They should do so either directly or by reporting the details to the managers of the central police system through which the information was provided.

6.13 The chief officer responsible for the police information concerned should then consider – and if necessary, record – any additions or changes to the recorded police information.

6.14 Where the recipient is outside the UK, the responsible chief officer must ensure that the conditions set out in section 78 of the DPA are in place.

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

Follow us
@CollegeofPolice

C00310121