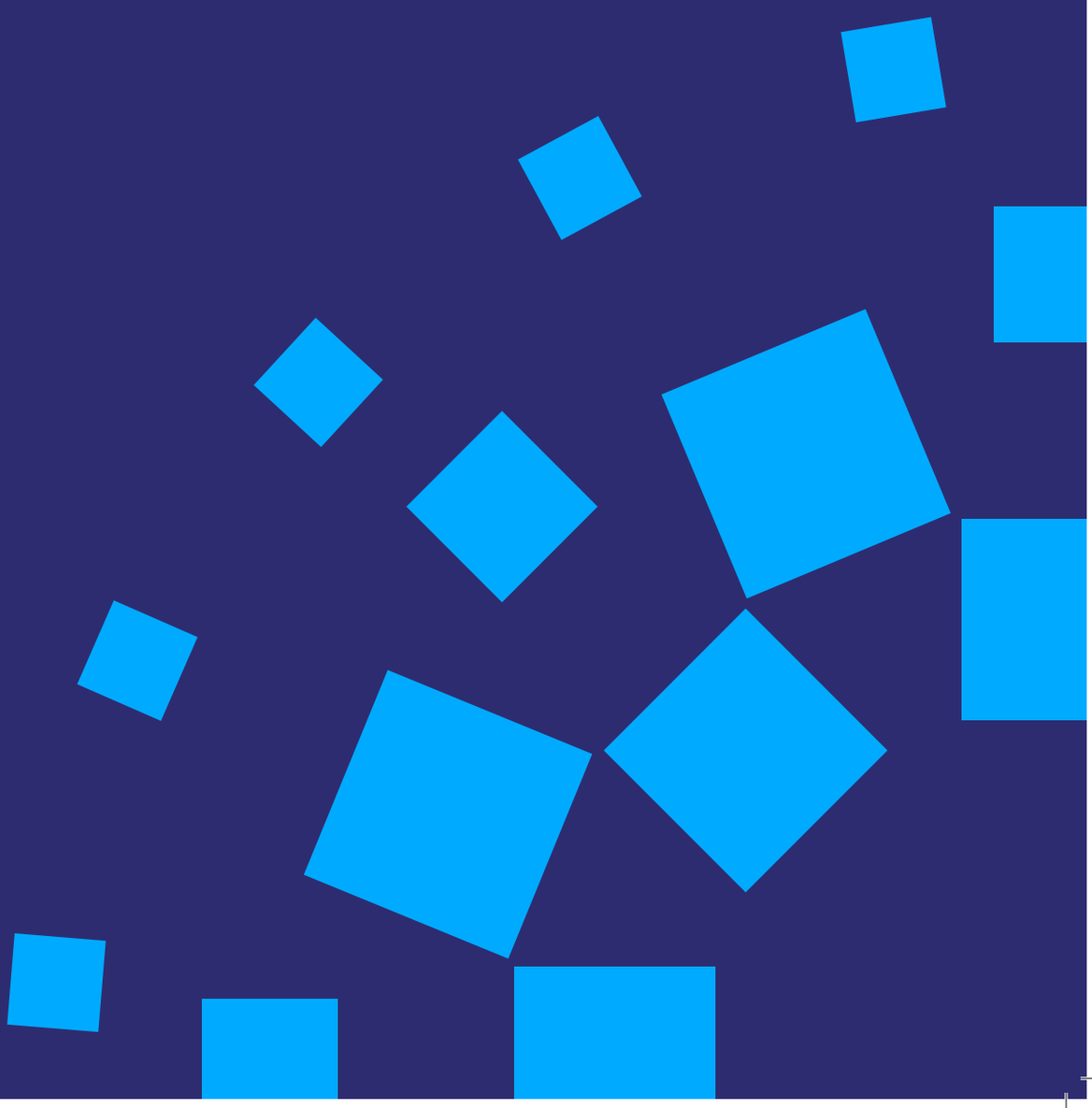
College of Policing

Working together to keep people safe

# Code of Practice on police information and records management

## July 2023



College of Policing

# Code of Practice on Police Information and Records Management

Presented to Parliament pursuant to Section 39A(5) of the Police Act 1996, as amended by Section 124(5) of the Anti-social Behaviour, Crime and Policing Act 2014

July 2023

This publication is available at **www.gov.uk/official-documents**.

Any enquiries regarding this publication should be sent to us at **contactus@college.police.uk**

ISBN 978-1-5286-4281-1

E02936199 07/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

# Contents

# 1 Introduction

1.1 Information and records management is an organisational function performed for the effective management of information throughout its lifecycle (creation, use, retention, appraisal and disposal), and across all aspects of policing. It is a function that is vital to delivering the core priorities of the service: to protect the public and reduce crime.

1.2 The nature of police information is constantly changing as new technology becomes available. Each new technology presents new ethical and legal issues, and should be supported by bespoke guidance. However, all police information, both operational and corporate, should be managed throughout its lifecycle in accordance with this Code.

1.3 Information recorded by police forces, all of which is subject to this Code, broadly fall into two categories: police corporate and police operational information. Both categories can include information that relates to an identified or identifiable individual, which constitutes personal data. Police forces processing personal data must do so in accordance with the relevant data protection legislation, the Data Protection Act 2018 (DPA 2018) and/or the General Data Protection Regulation (UK GDPR).

1.4 However, all records, whether containing personal data or not, must be managed in accordance with the principles in this code. The two categories of information are defined as follows.

1.5 Police corporate information is information that is processed to enable the discharge of police services, such as financial information, policies and procedures, and information relating to employees, such as personnel and disciplinary records.

1.6 Police operational information is information that is recorded for a policing purpose, mainly – but not exclusively – for:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice

- any other police duty or responsibility arising from common or statute law

1.7 It should be noted that the range of policing purposes are wider than the following definition of law enforcement purpose, which is provided for in section 31 of 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.'

1.8 This wider concept of policing purpose reflects the fact that the policing task extends beyond law enforcement.

1.9 The majority of police operational information will contain personal data and will be processed for law enforcement purposes, so it will be subject to the requirements of Part 3 of the DPA 2018. However, some personal data processing activities will be considered general processing subject to the UK GDPR.

1.10 The core principles for processing all types of information that become a record are broadly similar for the two categories. However, the nature of recorded police operational information requires extra safeguards to be in place, which are reflected in this Code and supporting national guidance.

1.11 Consequently, it is important to distinguish between information recorded for a policing purpose and information required for corporate functions that support the service to deliver.

1.12 Covert material contained within police records may be subject to additional safeguards contained within the Investigatory Powers Act 2016, Regulation of Investigatory Powers Act 2000 and associated codes of practice.

1.13 Any reference to police information in this Code (or just information) relates to both categories of information, namely operational and corporate, and may or may not include personal data.

1.14 Information must be recorded and records must be created when it is necessary for a police operational or corporate purpose. Forces should

capture sufficient technical and contextual information (metadata) to be able to:

- handle and control their information
- determine access
- 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.

1.15 The recording of police information should adhere to the separate Authorised Professional Practice (APP) that supports this Code[1].

1.16 To carry out the functions of policing, forces have to manage information from a range of sources and in a number of different forms (for example, digital, paper, biometric).

1.17 References to records may refer to any particular format or media, including (but not limited to):

- records containing biometric information
- hard copy records, including (but not limited to):
  - paper
  - microfilm
  - microfiche
  - DVDs
  - audio and video tapes
- digital records, including (but not limited to):
  - databases
  - audio and video
  - information created on mobile devices
  - spreadsheets
  - word-processed documents
  - email messages

1 Information Management APP

# 2 Purpose of the Code

2.1 The report of the Hillsborough Independent Panel (HIP) in 2009 and the report on the experience of Hillsborough families in 2017 expressed concerns that the management of police records and information was variable and inconsistent. This, in turn, had affected their ability to fully investigate the matters under consideration. This Code seeks to address the issues relating to the management of police information and records identified in the above reports.

2.2 This Code replaces the Management of Police Information (MoPI) Code of Practice 2005. It broadens the applicability of the original MoPI Code beyond records that contain police operational information to include police corporate information. It also updates the Code in light of related legislative and other developments. The Code also seeks to ensure consistency in the way forces archive records in the public interest.

2.3 The purpose of this Code is to:

- set national principles for police information and records management
- provide a template against which information management audits can be based
- provide guidance around the functionality necessary when developing new IT systems

It provides a framework to support a cohesive, ethical, effective and lawful approach to the management of all information and records within the police service. This, in turn, will maximise the opportunities and benefits that good information and records management provides.

2.4 This will improve accountability and increase the public's confidence in the way that information is managed by police forces.

2.5 The management of information and records in policing is already subject to a number of statutory obligations and standards. This Code builds on existing legal requirements for managing information and records, and must be considered in conjunction with all relevant legislative and regulatory requirements. In relation to personal data, in particular, this includes the statutory requirements set out in the

UK GDPR and DPA 2018. Although the UK GDPR and DPA 2018 underpin the Code in relation to records containing personal data, its purpose is wider than just meeting data protection requirements and it encompasses management throughout a record lifecycle.

2.6 This Code should be considered alongside other codes of practice that relate to different aspects of information and records management, such as (but not limited to), the codes of practice on:

- the Police National Computer (PNC) and Law Enforcement Database (LED)
- the Police National Database (PND)
- the management of records issued under Section 46 of the Freedom of Information Act (FOIA) 2000
- the ICO Code of Practice on data sharing

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

2.8 National complementary supporting guidance will provide advice on how this Code should be implemented to ensure compliance. This supporting guidance will be issued by the College of Policing in the form of APP, by the National Police Chiefs' Council (NPCC), by the Home Office and/or by national regulatory bodies such as the ICO.

## Role of other agencies in overseeing the code.

2.9 HMICFRS monitors and reports on the efficiency and effectiveness of the police, with the aim of encouraging improvement. HMICFRS can audit the way that forces manage information and records as part of their annual thematic reviews, if this is determined as a priority issue.

2.10 The ICO is the independent regulatory authority responsible for upholding information rights in the UK, most prominently the UK 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. The ICO will consider compliance with the Code as part of their wider data protection audits where records management falls within scope.

2.11 The College of Policing will publish the Code and, with the approval of the Home Secretary, may revise it where required, in whole or part, ensuring that it remains accurate and relevant for policing. The College will also publish supporting guidance referred to throughout this Code.

2.12 The NPCC will oversee police records and information management nationally, publishing policy and supporting guidance as necessary.

2.13 Police and crime commissioners (PCCs), and equivalents, have a duty to hold chief constables to account for the exercise of all their functions, including management of police information and records.

# 3 Statutory basis of the Code

3.1 This Code of Practice was issued on 20 July 2023.

3.2 The Code of Practice on Police Information and Records Management ('the Code') has been issued by the College of Policing with the approval of the Secretary of State for the Home Department. It is made under section 39A of the Police Act 1996, which allows the College of Policing, with the approval of the Secretary of State, to issue codes of practice relating to the discharge of their functions by chief officers of police if the College considers that:

a. it is necessary to do so in order to promote the efficiency and effectiveness of police forces generally

b. it is necessary to do so in order to facilitate the carrying out by members of any two or more police forces of joint or coordinated operations, or

c. it is for any other reason in the national interest to do so

3.3 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

3.4 In discharging any function to which the code of practice relates, a chief officer of police must have regard to this code.

3.5 The Code may be considered in a court of law and referenced in disciplinary proceedings. The Code will be considered by those who hold users to account for data management practice in a law enforcement or safeguarding context – for example, the Information Commissioner's Office (ICO) or the Independent Office for Police Conduct (IOPC).

3.6 Chief officers should ensure that anyone under their direction and control who uses information does so in accordance with the standards, as set out in the Code and the relevant legislation. Chief officers should also ensure that those users are aware of the potential consequences should they fail to act in accordance with the standards, as set out in the Code or the relevant legislation.

# 4 Key principles governing the management of police records and information

4.1 The following principles govern management of all police information and records, so while there is some similarity, these principles apply to a wider category of data than the data protection principles provided for in the DPA 2018. When processing personal data, chief officers should also have regard to national guidance on the DPA principles.

4.2 Creating and managing police 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 purpose for which it was collected
- is periodically reviewed, to ensure that it is retained for no longer than is required for the purpose for which it was recorded
- helps forces manage risk, protect the vulnerable and bring offenders to justice

4.3 The value of police 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

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

## Principle 1: Governance

4.5 Chief officers should ensure that their force has appropriate governance arrangements for police information and records management, including accountability and ownership. The chief constable or Commissioner, as 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.

4.6 Chief officers 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). The DPO role is a requirement under Article 37 of the UK GDPR and section 69 of the DPA 2018.

4.7 Chief officers should ensure that force governance arrangements, through the force SIRO, incorporate information risk and include clear routes for escalation. They should ensure that plans are in place to manage information breach incidents, including cyber incidents, effectively. The plans should emphasise the importance of assessing and mitigating the risk associated with the breach and the recovery options available when material is unlawfully disclosed.

4.8 Chief officers should ensure that individual post-holders are in place with responsibility for records management, information security, data protection and freedom of information on a day-to-day basis.

4.9 Strategies and tactical plans should be developed to embed good practice. Chief officers should promote an environment and culture whereby both the benefits and the responsibility of holding personal

data are understood, ensuring that access, processing and retention is legitimate and lawful.

4.10 Chief officers should ensure development and application of a consistent classification scheme or taxonomy, in order to organise and index records to facilitate easy retrieval.

4.11 Records created and acquired during the performance of duty, and any duplicates and copies of these records, remain the property of the force. Chief officers should ensure that their force has systems and processes in place to ensure that these records are accounted for when individuals leave the organisation.

4.12 Chief officers should establish and maintain information and records management policies within their forces that comply with supporting national guidance and the principles of this Code.

4.13 Chief officers should assess their policies and procedures against the requirements of the Code and associated guidance at regular intervals, and update them if necessary. Risks associated with non-compliance should be included in the force's risk management framework.

## Principle 2: Transparency

4.14 Chief officers must ensure that, where appropriate, their force is transparent[2] with the public about the nature and type of the records and information they hold, and how and why their information is being processed. To assist in this, they must publish a privacy notice in line with the guidelines published on the ICO website.

4.15 In relation to personal data that is not processed for a law enforcement purpose, Article 5 of the UK GDPR requires forces to process it 'lawfully, fairly and in a transparent manner in relation to individuals'.

4.16 However, the equivalent principle in section 35 of the DPA 2018, which covers processing for law enforcement purposes, does not include the requirement for transparency. This is due to the potential to prejudice an ongoing law enforcement investigation in certain circumstances, which means full transparency may not be possible.

2 Set out under the controller's general duties in section 44 of the DPA 2018.

4.17 Transparency should not overrule necessary operational and personal confidentiality. While police information that has been obtained covertly should be managed in the same way as other records, in that they are reviewed and deleted once there is no longer a policing purpose for their continued retention, the release of such information should be considered on a case-by-case basis in line with the DPA 2018 and ICO guidance.

## Principle 3: Quality

4.18 Chief officers should be proactive and commit to driving improved information quality to achieve confidence and consistency, improve decision-making and protect the public from harm. They should communicate the importance of improving information quality and the adoption of behaviours to place quality at the forefront of activities concerning data, information and records.

4.19 All staff should be made aware of their responsibility for the quality (accurate, adequate and not excessive) of the information they process. Police information and records must be created and managed in accordance with national standards (such as the National Crime Recording Standards and the National Standards for Incident Recording), guidance and statutory obligations.

4.20 Chief officers should ensure that the design and maintenance of information and records systems take account of the stages of the lifecycle, ensuring ongoing accuracy, reliability, integrity and usability, and making sure that subsequent value is not compromised.

4.21 Chief officers should adopt practices to anticipate changes in technology, processes and people that will affect information quality standards. Chief officers should integrate information quality standards into the design of new systems and processes.

# Principle 4: Compliance

4.22 Chief officers should put arrangements in place to ensure that information is handled in line with relevant legislative and regulatory obligations, including the supporting national guidance.

4.23 Automated systems used to process personal data under the DPA 2018 Part 3 (law enforcement) must meet the logging requirements set out in section 62 of the Act.[3]

4.24 Police operational information should undergo evaluation appropriate to the policing purpose for which it was collected and recorded[4]. All police operational information should be evaluated to determine:

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

4.25 Chief officers should ensure that force IAOs are aware of their force's obligations to manage information and the metadata appropriately, including retention, disclosure, preservation and disposal. Disposal can be either transfer to an archive or appropriate secure destruction.

4.26 The principles 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.

4.27 A 'data protection by design and default' approach[5] must be built into planning for new processing activities, as well as for changes to processing activities. The opportunity to implement automation of review, retention and disposal processes should also be considered.

3 For automated processing systems set up before 6 May 2016, the logging requirements in section 62 must be complied with by 6 May 2023. This is provided for in paragraph 14 of Schedule 20 to the Act.

4 Information Management APP.

5 Section 57 of the DPA 2018.

4.28 The purpose of any information technology asset, and the criteria against which personal data will be recorded onto it, must be clear and defined to avoid any ambiguity or ad-hoc recording.

4.29 Where possible, the existence of the asset should be publicly known, along with the criteria above (paragraph 4.28). The information held on it should be searchable and accessible, to enable individuals to exercise their data protection rights, such as appropriate right of access[6].

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

4.31 Chief officers should put in place policies, procedures and control measures to protect information and personal data from:

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

4.32 The force DPO should be given the responsibility for monitoring the compliance with the policies of the controller, in relation to the protection of personal data.[7]

4.33 Chief officers should – through measures such as self-assessment tools, external assessments, peer reviews and accreditation schemes – be able to demonstrate that their information and records management practices comply with the standards detailed in this Code and their force policies. They should develop plans to address shortfalls and pursue continuous improvement.

4.34 When a third party is used to process personal data (corporate or operational) on behalf of a force, or when joint controller arrangements are in place[8], suitable checks must be undertaken to ensure the third party's reliability. Contractual arrangements must be in place, in line with the guidance included on the ICO website.

6 Section 45 of the DPA 2018.

7 Section 71 of the DPA 2018.

8 Sections 58 and 59 of the DPA 2018.

## Principle 5: Accessibility

4.35 Chief officers should ensure that force systems used to manage information and records have the functionality necessary for adherence to the principles in this Code.

4.36 Chief officers should ensure that access to information is only given to authorised individuals who need access for their lawful function.

4.37 Chief officers should ensure that systems are in place that make it easy to understand what information the force holds. The information should be stored in a way that ensures its efficient retrieval. In the case of records containing personal data, chief officers must ensure that their force has a formal, documented, comprehensive and accurate record of processing activities (ROPA)[9] based on a data mapping exercise that is reviewed regularly.

4.38 Chief officers should ensure that business continuity arrangements and disaster recovery plans are 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

4.39 Chief officers should implement the appropriate review and retention procedures and periods in line with national guidance, including College information and records management APP, guidance relating to specific material (such as covert, biometric and evidential material), and any retention schedule published by the NPCC.

4.40 Chief officers should ensure that retention of information is the product of a deliberate and purposive decision, rather than a default position of non-deletion. Deliberate, purposive retention should also be supported by IT systems that enable careful, timely decisions to be taken in a way that supports the lawfulness and ethical elements of this Code.

4.41 Chief officers should ensure that records that need to be preserved for future use should, wherever possible, be migrated to newer formats

9 Section 61 of the DPA 2018 and Article 30 of the UK GDPR require organisations to create and maintain a record of processing activities (ROPA).

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.

4.42 Where a decision is made to retain a record for longer than the designated retention period, the justification and lawful basis for the extended timescale must be recorded.

4.43 Chief officers should put arrangements in place for the selection of records for permanent preservation, as well as records subject to ongoing and announced public inquiries, in line with associated guidance[10].

4.44 Under the Inquiries Act 2005, chief officers may be required to preserve relevant records for the inquiry for as long as necessary. The obligation to retain and not alter or destroy relevant documents will remain for the duration of an inquiry.

4.45 Chief officers should ensure that information and records are only retained for as long as there is a legitimate corporate or policing purpose, while being cognisant, in line with national guidance, of records where wider public interest, statistical, scientific or historical purposes may necessitate extended or permanent retention.

4.46 When archiving records containing personal data, chief officers should be cognisant of the legal safeguards in the following sections of the UK GDPR and DPA 2018:

- Article 89(1) of the UK GDPR
- section 19, Part 2 of the DPA 2018 (general processing)
- section 41, Part 3 of the DPA 2018 (law enforcement processing)

## Principle 7: Disposal

4.47 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 disposal. These may include secure destruction or archiving in the public interest for historical or scientific purposes.

10 Archiving in the Public Interest APP.

4.48 Chief officers should ensure that arrangements are in place to be able to explain why information is no longer held, either by reference to a record of its destruction or by reference to the force's policy.

4.49 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 (for example, putting beyond use or restricting access) while a force works towards a suitable IT solution.

4.50 Chief officers should ensure that arrangements are in place to archive selected documents for permanent preservation, in line with national guidance, where they are no longer required for a corporate or policing purpose. This may be in partnership with an external archive service.

4.51 Archived physical records, such as paper and microfiche, should comply with the relevant care and conservation standards, as detailed in national guidance issued by the British Standards Institute.

4.52 In the case of digital records that meet the criteria for archiving, 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.

4.53 Chief officers who choose to archive records for permanent preservation with an external provider should agree governance arrangements through a data processing contract. This agreement should:

- identify, among other things, the controller
- clarify who is responsible for freedom of information and data protection obligations
- outline a process for recalling records

4.54 Chief officers should keep details of records that have been permanently archived, including detail relating to the nature of the record, their context and their location.

# 5 Organisational requirements

## Personnel capability

5.1 Chief officers should identify the key posts that they recognise as being required for the management of police records, and should ensure that the posts are filled and the function is suitably resourced. To ensure standards of competence, chief officers should also arrange appropriate 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. Chief officers should ensure that all staff understand their individual responsibility for how they process and handle information.

5.3 Training for managing records and information management is not only to support 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 relevant legislation and to follow the principles in 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 Chief officers should comply with the ICO Code of Practice on data sharing when sharing personal data. Data 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 UK GDPR and Part 2 of the DPA 2018.

6.2 The UK GDPR and DPA 2018 provide a framework to ensure that the sharing of personal data is done in a fair, lawful, proportionate and secure way. It should not be perceived as a barrier to appropriate information sharing. Appropriate information sharing can be beneficial for society as a whole and it can sometimes be more harmful not to share information.

## Sharing of police information within the UK police service

6.3 Chief officers should ensure that information recorded for policing purposes, as well as any assessments of its reliability, should be made available to any other police force in England and Wales that legitimately requires the information for their policing purposes. However, this is subject to any requirements arising from legislation. Further guidance is available from the national information sharing APP and the Information Commissioner's Data Sharing Code of Practice. Sharing police information containing personal data must be lawful, proportionate and necessary.

6.4 Other police forces in the UK should be afforded the same degree of access to information that has been recorded for policing purposes by police forces in England and Wales. However, this is subject to the same requirements 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 and data protection legislation (where personal data is being requested).

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 high-quality data to national systems

## Sharing of police information with UK-based non-law enforcement agencies

6.6 Chief officers should ensure that there are processes in place to allow the sharing of police information with non-law enforcement bodies when there is a legal basis to do so.

6.7 In cases where information is shared on a regular basis, formal arrangements should be made through the development of data-processing contracts, Memoranda of Understanding (MoU), 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 UK GDPR, provided that the processing has a clear basis in law[11].

## Sharing police information outside the UK

6.9 Chief officers may arrange for law enforcement authorities outside the UK to receive both police operational and corporate information, on request, 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 personal data is to be transferred to forces outside the UK for a law enforcement purpose, chief officers must apply the criteria contained within sections 72 to 78 of the DPA 2018 before agreeing such a request. Before transference, chief officers should also take into account any relevant guidance issued by the ICO.

11 Section 36(4) of the DPA 2018.

## Sharing of sensitive police operational information and sources

6.11 National guidance[12] provides for special procedures to be applied to a request for access to information recorded for policing 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 Chief officers should make sure that those receiving information are aware of their responsibilities. In making national or local agreements and protocols for the sharing of information with people or bodies other than police forces, or in responding to individual requests for information outside such agreements or protocols, chief officers should consider the legal requirements contained within the UK GDPR and DPA 2018. Guidance is available from the national information sharing APP and the Information Commissioner's Data Sharing Code of Practice and supporting guidance.

6.13 If a person or body who requests 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.

12 Data Protection Manual of Guidance.

# 7 Glossary of terms

### Authorised Professional Practice (APP)

APP is developed and owned by the College of Policing and can be accessed online. It is the official and most up-to-date source of policing practice. It is part of the supplementary guidance available to forces to help implement the Code.

### Data

Data consists of raw figures and facts collected by an organisation in the conduct of its business.

### Government Security Classification

How the government classifies information assets to ensure they are appropriately protected. This approach has been adopted by the police service.

### Information

Information is data that is processed, organised, structured or presented in a given context so as to make it useful.

### Metadata

Data that provides information about other data.

### Personal data

Personal data is defined in section 3 of the DPA 2018 as any information relating to an identified or identifiable living individual. An identifying characteristic could include a name, ID number or location data. Such information should be treated as personal data, even if it can only be potentially linked to a living individual.

### Police corporate information

Police corporate information is information processed to enable the discharge of police services, such as financial information, policies and procedures, and information relating to employees, such as personnel and disciplinary records.

## Police operational information

Police operational information is information recorded for a policing purpose, mainly – but not exclusively – for:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice
- any other police duty or responsibility arising from common or statute law

## Supporting guidance

National complementary supporting guidance will provide advice on how this Code should be implemented to ensure compliance. This supporting guidance will be issued by the College of Policing in the form of APP, by the National Police Chiefs' Council (NPCC), by the Home Office and by national regulatory bodies, such as the ICO.

E02936199
978-1-5286-4281-1