



**Policy Title** MoPI – Review, Retention and Disposal Policy  
**CCMT Sponsor** Director of Information, Science and Technology  
**Department/Area** Information Management Department  
**Section/Sector**

---

## **1.0 Rationale**

## **2.0 Intention**

## **3.0 General Principles**

## **4.0 Guidance, Procedures & Tactics**

## **5.0 Challenges & Representations**

## **6.0 Communication**

- 6.1 [Links to Police National Legal Database/Other](#)
- 6.2 [Implementation Strategy \(Policy Impact Assessment\)](#)

## **7.0 Compliance and Certification**

- 7.1 [Human Rights Audit](#)
- 7.2 [Diversity Impact Assessment](#)
- 7.3 [Diversity \(Human Resources\)](#)
- 7.4 [Management of Police Information \(MoPI\)](#)
- 7.5 [Community Engagement Standards](#)
- 7.6 [Data Protection](#)
- 7.7 [Freedom of Information Act](#)
- 7.8 [Protective Markings](#)
- 7.9 [Health & Safety at Work](#)

## **8.0 Monitoring and Review**

## **1.0 Rationale**

- 1.1 This policy specifies the Force approach, business rules and responsibilities for the process of Review, Retention and Disposal (RRD) of Police Information in accordance with the Management of Police Information (MoPI).
- 1.2 This policy has been drawn up within the context of:
- Management of Police Information (MoPI) Code of Practice 2005 (CoP)
  - Guidance on MoPI 2006
  - MoPI Threshold Standards
  - Force Information Management Strategy
  - Force Risk Management policy
  - And links with other legislation, statute and common law, regulations or national and local policies and procedures affecting the Force.

## **2.0 Intention**

- 2.1 The primary purpose of RRD is to help manage the risk posed by known offenders and other potentially dangerous people by ensuring that Police Information relating to such people is well managed and of good quality. Police Information is that required for a policing purpose and legal duty. The MoPI Guidance defines policing purpose as:
- Protecting life and property
  - Preserving order
  - Preventing the commission of offences
  - Bringing offenders to justice
  - Any duty or responsibility arising from common or statute law.
- 2.2 Reviewing information to determine its accuracy, adequacy and continuing necessity for a policing purpose is a reliable means of ensuring it is held lawfully in compliance with the Data Protection Act (DPA). Review procedures minimise the risk of censure by the Information Commissioner by enabling the Force to demonstrate that information is managed appropriately and retained proportionately. Review procedures will also help prevent the Force being overloaded by the volume of information captured and recorded, and the costs associated with increasing storage requirements.
- 2.3 Additionally, a failure to review and retain information appropriately may constitute a breach of legislation and, ultimately undermine public confidence in the police service.

**3.0 General Principles** 3.1 The key MoPI principles to be applied are:

- The review of Police Information is central to risk-based decision-making and public protection
- Records will be reviewed in line with this policy in order to ensure that they remain necessary for a Policing Purpose, are adequate, up to date and are subject to review as per the review schedule
- The type and amount of information held on an individual must not be excessive and will be proportionate to the risk they pose
- There is a presumption in favour of the retention of police information providing the preceding principles are met
- Records will be disposed of when there is no longer a Policing Purpose for retaining them. Records initially identified for disposal may be retained where there is a documented rationale
- The review process will be documented for audit purposes.

3.2 The Force will apply additional principles of:

- Data quality and risk assessment at the point of input are critical to ensuring the overall Force goal of information being fit for purpose and to the freeing of scarce resources to focus on high-risk offenders
- Person Records for review will be prioritised according to risk and to the agreed priorities prevailing at any point in time, for which business rules and guidelines will be maintained and made available to review staff
- Where the risk level so justifies, Person Records may be assessed automatically by a computer system, applying business rules as would be applied through a manual review. Exceptions that cannot be addressed automatically will be queued for manual review.

**4.0 Guidance, Procedures & Tactics**

**4.1 Scope**

4.1.1 This policy applies to all police information as defined in the MoPI CoP and Guidance. For the purposes of this policy this means Person Records held for a policing purpose in specific Force systems within the priority business areas identified by IMPACT:

- Crime
- Intelligence
- Criminal Justice (Custody)
- Domestic Violence
- Child Protection
- Firearms.

## **NOT PROTECTIVELY MARKED**

4.1.2 The objectives to be addressed by the Force's RRD processes are to:

- Maintain and manage a work queue of Persons for review prioritised according to risk and the prevailing Force priorities as may apply at any point in time
- Review Persons on this list and assign or amend the MoPI Risk Group for the Person
- Set or reset the scheduled review date for a Person
- Verify Person Records are linked to other forms of information (Person; Object; Location; Event)
- Identify records for correction, amendment or disposal; to be actioned by nominated data owners
- Log new information found for intelligence purposes, to be actioned by intelligence staff and to forward Persons of concern to operational units for evaluation
- Identify Person Records for disposal and confirm their disposal.

4.1.3 When the Police National Database (PND) becomes available the RRD Policy will be amended to include interaction with this system, once the Force has considered the impact and responded.

4.1.4 Exclusions from the scope of RRD are:

- Information processed for purposes connected with the administration of the Force and its employees is not included
- Police Information held in designated systems not part of priority business areas, not within core IT applications and not within the scope of the priorities defined by the IMPACT Programme (see 4.1.1 above)
- Police Information held in magnetic, photographic and optical formats and on paper is not included in this version of the RRD Policy – they will be managed by individual Retention Schedules
- Police information held in confidential areas; Special Branch/Counter Terrorism Unit and Professional Standards Department. These business areas are responsible for the review, retention and disposal of the information they hold
- Person Records held on the Police National Computer (PNC). This is covered by the 'Retention Guidelines for Nominal Records on the PNC', which are available from the ACPO web site.

## **4.2 Remit to deliver the policy**

4.2.1 The Force Records Manager is responsible for delivering and maintaining the RRD policy and processes and for ensuring they are delivered by the RRD Review Team Manager.

4.2.2 The RRD Review Team will perform the RRD procedures.

4.2.3 Data management of source information including the resolution of data issues and the addition of new information is the responsibility of the business area and system owners. Issues identified for action

## **NOT PROTECTIVELY MARKED**

## NOT PROTECTIVELY MARKED

during a review action will be forwarded to the nominated roles in these areas.

- 4.2.4 Every member of the Force has a responsibility to be aware of this RRD policy and to contribute to its effectiveness by ensuring that information is recorded and evaluated correctly from the outset.

### 4.3 The Procedures

#### 4.3.1 Establishing a MoPI Risk Group

- The MoPI Guidance lists three Risk Groups for Persons who have offended or who pose a risk of offending:
  1. The most serious group; the risk relates to Certain Public Protection Matters – serious sexual and violent offences
  2. Other sexual and violent offences
  3. All other offences
- The requirement is to categorise records into their MoPI Risk Groups for RRD purposes. Risk relates to a person and not to an individual record and is determined by assessment of all relevant Police Information relating to a Person
- Risk Groups have been determined at the national level by the NPIA and are based on a mapping of Risk Groups to Home Office Offence Codes. This mapping has also been published on the PNLD Database. The Force has mapped Risk Groups to intelligence categories and reasons for arrest, using the NPIA/PNLD Home Office Offence Code mapping as a basis
- Past behaviour is an indicator of future behaviour and the offence an offender, alleged offender or suspect is linked to is a clear indicator of risk. Suspicion is to be derived from intelligence and crime investigation.
- The highest risk group indicated by the information available at the time of the review will be applied. If a subsequent event or new information would amend the risk categorisation this will be addressed either by a review triggered by the new event or information or, at the latest, by the next scheduled review.
- When searching information to determine which MoPI risk category will apply to a person, the first instance of an offence or intelligence found that categorises the person as Group 1 is sufficient. However a review of all records may be required to verify linking, adequacy and quality.
- Information for a Group 2 person may be retained where it is not linked to serious specified offences in the Criminal Justice Act as long as the offender or suspect is confirmed as posing a risk of harm according to the National Retention Assessment Criteria (NRAC) and/or continues to offend
- Records relating to “non-innocent” Persons not falling with Group 1 or Group 2 are dealt with as Group 3. Where there is concern that a Group 3 poses a more serious risk they may be assessed as

NOT PROTECTIVELY MARKED

## **NOT PROTECTIVELY MARKED**

being a Group 3 Exception and will be updated to Group 2. The rationale for this will be recorded using the NRAC.

### **4.3.2 Review Person Records**

- Records identified for review will be actioned in priority order, based on risk. The currently active list of priorities will be maintained as part of the RRD guidance and procedures
- The review will assess the Risk Group applicable to the Person, identify whether the Person or any related records should be disposed of and inspect overall quality of the information
- Where there is concern that Police action may be required or where new information has come to light, this will be forwarded by the Review team using standard Intelligence procedures
- Where a review identifies data quality or duplication issues to be actioned these will be passed to the business owner of the records in question for action
- The RRD Review Team will provide feedback wherever there are concerns about the quality of the information being recorded or the evaluation procedures undertaken
- All reviews must be recorded for audit purposes and the Reviewer will log the date of review, the reviewer's name, the outcome and the reason for the decision taken. This will be supported by the completion of a MoPI National Retention Assessment Criteria (NRAC) form. A future review date will be set according to the Review Schedule.

### **4.3.3 Retention and Disposal**

- Where the review process and application of the National Retention Assessment Criteria results in a decision to retain information, the review will be authorised by the RRD Reviewers. Retention decisions will be subject to dip sampling quality checks by the RRD Review Team Manager
- In the event that the outcome of a review suggests that a record should be disposed of, according to NRAC criteria, but the Force has other reasons for believing that the record continues to be necessary for a policing purpose, the decision to retain this record will be authorised by the nominated manager from the owning business area
- For Group 1 or 2 Person Records where disposal is indicated, the decision will be authorised by a senior manager: Group 1 deletions to be authorised at Superintendent level; Group 2 deletions to be authorised at DCI level; Group 3 deletions will be authorised by the RRD Review Team Manager. An authorisation matrix will be maintained by the RRD Review Team Manager, mapping Risk Groups and Offender categories to the appropriate rank and business area
- Records will not be disposed of where the Person is marked as being of special interest. Once the marks are removed, the Person will be subject to a review as normal.

**NOT PROTECTIVELY MARKED**

#### **4.3.4 Audit**

- All Person Records marked for disposal following the review process will be disposed of in accordance with the ACPO/ACPOS Information Systems Community Security Policy and with the Force Security Policy
- The RRD Review Team Manager will conduct sample quality checks on a monthly basis of reviews undertaken to ensure quality
- A central audit role, independent of the RRD Review Team will conduct an annual inspection of Force Person Records to ensure ongoing compliance with this policy
- A secure audit trail for all reviews will be maintained.

#### **4.4 Remit for management of the policy**

4.4.1 Responsibilities for the management of the policy are:

- The Force Information Officer is responsible for ensuring the RRD policy remains fit for purpose and is consistent with the Information Management Strategy, as directed by the Chief Information Officer

### **5.0 Challenges & Representations**

Head of Department (Job Title)/Area: Force Information Officer  
Full Address: Force Headquarters (South)

### **6.0 Communication**

#### **6.1 Links to Police National Legal Database Other**

Risk is assigned to a Person based on their links to offending or possible offending. Offences have been assessed by the NPIA and a MoPI Risk Group set for each. This list is maintained on the PNLD and forms the basis for the application of Risk by the Force.

#### **6.2 Implementation Strategy**

The implementation of the policy will require communication to selected roles within the Force:

- RRD Review Manager – to implement the policy
- Information Management Department Senior Management Team – to implement and maintain governance of the policy
- Data and Systems Owners who have responsibility for data administration – to be aware of the requirement to resolve data issues found as a result of RRD reviews
- Intelligence Teams – to receive new intelligence reports from the RRD Team where a review highlights a concern

## NOT PROTECTIVELY MARKED

- BCU/OCU Commanders – whose teams may, in future, receive from the RRD team feedback on the accuracy of data collected and recorded by their staff.

### 7.0 Compliance and Certification

#### 7.1 Human Rights Certification

The Human Rights Audit will be carried out by a trained [Human Rights Auditor](#).

#### Legal Basis

The requirement for this policy arises from the Code of Practice on the Management of Police Information (MoPI) 2005, made under the Police Act 1996 and 1997, and coming into effect on 14 November 2005. The Guidance on the Management of Police Information was published in 2006, under the Code of Practice and chief officers must have regard to both the Code and the Guidance.

The Guidance sets out the key principles that must be satisfied for Police Information to be managed legally.

#### Human Rights Articles Engaged

The MoPI Guidance makes particular reference to Article 8, which protects an individual's right to privacy and family life.

Audited by: (name)

Audited on: (date)

#### Prohibition of Discrimination

Does this policy have the potential to discriminate? If so, how and what are the mitigating factors?

#### 7.2 Diversity Impact Assessment

This policy has been assessed for its relevance to the six strands of Diversity and has been rated as '**LOW.**'

NOT PROTECTIVELY MARKED

## NOT PROTECTIVELY MARKED

### 7.3 Diversity (Human Resources)

In the application of this policy, the Force will not discriminate against any persons regardless of their gender, sexual orientation, race or ethnic origin, religion, age or disability.

### 7.4 Management of Police Information (MoPI) Compliance

This policy addresses Section 7 Review, Retention and Disposal of the MoPI Guidance.

### 7.5 Community Engagement Strategy and Standards

This policy has no community engagement implications.

For further information, please see the following links:

[Community Engagement Strategy](#)

[Standards](#)

### 7.6 Data Protection

The MoPI Guidance sets out the impact of the Data Protection Act for the management of Police Information. This includes reference to Section 29 which creates exemptions to certain data protection principles where data is processed or shared for the purposes of:

- Prevention or detection of crime
- Apprehension or prosecution of offenders
- Assessment or collection of any tax or duty.

### 7.7 Freedom of Information Act

In line with the Freedom of Information Act 2000 all policies which do not contain Police tactics and have the GPMS 'NOT PROTECTIVELY MARKED,' will be made available to the public. Any other [Exemptions](#) to this should be evidenced to prove why this policy should not be published, e.g. publishing this policy will:

- (i) Present a real risk of breach of security
- (ii) Impede the course of a criminal investigation

This policy is suitable for sharing with the public (to be confirmed).

### 7.8 Protective Markings

The policy has been classified as **NOT PROTECTIVELY MARKED**.

NOT PROTECTIVELY MARKED

### 7.9 Health & Safety at Work

It is considered that HSE legislation does not apply to this policy, therefore no risk assessments are required.

### 8.0 Monitoring and Review

The implementation of this policy is driven and assessed by the Force Action Plan for MoPI, a nationally defined plan.

A full review will be carried out by the policy author and will examine:

- Changes in legislation
- Court rulings – Domestic, European and Human Rights
- Examples of good practice from other Forces or other organisations
- Changes in Home Office Circulars
- Developments with ACPO Policy Unit
- Representations made by individuals and relevant organisations
- Relevant Equality data.

The policy will be reviewed when any of the above triggers occur or at least annually.

The next scheduled review of the policy is November 2010.

<u>Chief Officer Policy Authorisation</u>	
<b>Policy signed off by:</b>	
<b>Name of relevant ACC</b>	<b>Date</b>