

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

## **Military Police Investigative Doctrine**

### **Chapter 45 – The Management of Service Police Information**

#### **Publication Information**

Sponsor: SO1 PolCom  
Author: SO1 PolCom  
Last Updated: 23 Jan 17

Users are reminded that a document downloaded to their desktop or personal work area will not reflect subsequent updates made to versions published on the Provost Portal.

#### **Review Process**

**Stakeholder Review** – This document will next be reviewed in and on an annual basis thereafter by SO2B PM(A) and nominated representatives from SPCB.

**Legacy Audit Trail** – The following updates and amendments have been made to this chapter and previously published versions retained for audit purposes.

<b>Date of re-publication:</b>	<b>Paragraphs amended:</b>	<b>Actioned by:</b>

**Subject Matter Experts** – The College of Policing Authorised Professional Practice on Information Management provides best practice for the Service Police to follow.



## **Military Police Investigative Doctrine Chapter 45 – The Management of Service Police Information**

This Chapter contains information previously held under MPID 26, which was republished in December 2016 to focus on Archive Policy. Chapter 45 replaces the non-archiving elements of Chapter 26 and is currently under review. It will be updated during 2017.

The aim of this chapter is to define the Service Police Policy and provide guidance for the review, retention and destruction of Service Police documentation, in order to:

- a. Prevent the premature destruction of information.
- b. Provide consistency of preservation / destruction.
- c. Improve record management.

Archiving of Service Police Information will be carried out in accordance with MPID Chapter 26 – Archiving. All Service Police information held on electronic systems is subject to the same retention periods as hard copy archives.

This chapter applies to the Management of Service Police Information from 1 January 2009 onwards. All management prior to this date will continue to be regulated against Chapter 59 of the Provost Manual.

### **Index**

Section 1	Introduction		1.1 1.2 1.3	<u>Management of Police Information</u> <u>Service Police Information</u> <u>Legal Basis</u>
Section 2	General Principles		2.1 2.2 2.3	<u>Service Police Information</u> <u>Categorisation of Offences</u> <u>Clear Periods</u>
Section 3	Guidance Procedure and Tactics		3.1	<u>Service Police Information Groupings</u>
		First Response	3.2	<u>Retention</u>



~~OFFICIAL~~  
~~Handling Instruction: Limited Circulation~~

		Initial Actions	3.3	<u>Retention Assessment Criteria</u>
		Qualified Response	3.4 3.4.1 3.4.2 3.4.3 3.4.4 3.4.5 3.4.6 – 3.4.11	<u>Reviews</u> <u>Triggered Reviews</u> <u>Trigger Review Panel</u> <u>Documenting the Review Process</u> <u>Authorising the Review Process</u> <u>Inspections and Audits of Reviews</u> <u>Disposal</u>
		Regional Variations	3.5	<u>Regional Variations</u>
Section 4	Compliance and Qualification		4.1 4.2	<u>Qualification</u> <u>Recusal</u>
Section 5	References		5.1	<u>Reference – Legal</u>
		Associated Policy	5.2 5.2.1 5.2.2 5.2.3 5.2.4 5.2.5	<u>Associated Policies</u> <u>Annex A – Service Police Information Grouping</u> <u>Annex B – Listed offences against assigned Service Police Information Groupings</u> <u>Annex C – Service Police Retention Assessment Proforma</u> <u>NPIA Guidance on The Management of Police Information 2010</u> <u>JSP 441 – Defence Information Management Policy and Procedures</u>
Section 6	Training		6.1	<u>Training</u>
Section 7	Financial		7.1	<u>Budget Implications</u>
Section 8	Lessons Learnt		8.1	<u>Abrided Learning Account</u>

## Introduction

**1.1 Management of Police Information.** Effective policing is reliant on the efficient management of police information in order to protect the Service and wider civil community, prevent crime and bring offenders to justice. However, it is incumbent on the Service Police to balance this need to retain information with an individual's human rights and civil liberties. It is this balance of human rights versus public protection that this chapter addresses.

**1.2 Service Police Information.** For the purposes of this Chapter, Service Police information is classed as information that is required for a policing purpose. The Management Of Police Information (MOPI) Code of Practice<sup>1</sup> defines policing purposes as:

- a. Protecting life and property.
- b. Preserving order.
- c. Preventing the commission of offences.
- d. Bringing offenders to justice.
- e. Any duty or responsibility of the Service Police arising from common or statute law.

These 5 purposes also provide the legal basis for collecting, recording, evaluating, sharing and retaining Service Police information. It is

---

<sup>1</sup> ACPO Guidance on The Management of Police Information, Second Edition dated 2010.

essential that a policing purpose is established in order for the information to be legally held. The 5 policing purposes are not mutually exclusive. Information can be collected for one policing purpose and used for another.

**1.3 Legal Basis.** In order for Service Police information to be made available to support policing purposes, the legal framework should first be understood. This chapter highlights the key principles that should be satisfied for Service Police information to be managed lawfully; it does not set out the legal framework in detail, however establishing a policing purpose is the key principle which underpins the retention of Service Police information. The information must have a policing purpose if a lawful basis for holding it is to be established. If there is no policing purpose then the information cannot be held as police information. Legal References in relation to this Chapter are contained within [Para 5.1](#).

## General Principles

**2.1 Service Police Information.** Service Police information consists of conviction and non-conviction data. It is important that non-conviction data, in particular, is not treated as fact and is handled with the utmost sensitivity.

**2.2 Categorisation of Offences.** The Categorisation of offences focuses on those offenders who present a risk of harm because of the seriousness of their offences. It also acknowledges that a risk of harm may be presented by potentially dangerous people who have not yet been convicted or even accused of serious offending, but whose behaviour nonetheless, causes concern. Additionally, prolific offenders

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

whose criminal activity is lower level, but higher in frequency, also pose a risk of harm to the public and Service community. Information about them may therefore, need to be retained for as long as they continue to engage in criminal activity.

**2.3 Clear Periods.** A Clear Period is defined as the length of time since a person last came to the attention of the police as an offender or a suspected offender, for behaviour that can be considered a relevant risk factor. The use of designated clear periods enables the Service Police to retain information relating to prolific offenders for as long as they continue to offend, while allowing for the removal of information not required for a policing purpose. The triggered review process will ensure that information relating to prolific offenders remain adequate and up to date. Further information on triggered reviews is contained in [Para 3.4.1](#).

## Guidance, Procedure & Tactics

**3.1 Service Police Information Groupings.** Service Police information is divided into 4 groups:

- a. **Group 1 – Certain Public Protection Matters.** The Service Police acknowledge that there are certain public protection matters which are of such importance that information relating to them should only be disposed of if it is found to be entirely inaccurate or no longer necessary for a policing purpose. Group 1 includes information /offences relating to:

1. [Multi-Agency Public Protection Arrangements \(MAPPA\)](#) managed offenders.
2. [Serious offences specified in Criminal Justice Act 2003 \(CJA 03\)](#)<sup>2</sup>, historical offences that would be investigated as such today or Service offences which could be investigated as a serious offence under CJA 03.
3. Potentially dangerous people<sup>3</sup>.
4. Any offence under [Schedule 2 \(AFA 06\)](#), (JSP 830, Manual of Service Law).

The Service Police may retain all information relating to Certain Public Protection Matters until such a time as the **subject has reached 100 years of age**. There is still a requirement, however, to review this information regularly to ensure it is adequate and up to date. This must be done every 10 years.

- b. **Group 2 – Other Sexual, Violent or Serious Offences.** This Group includes the following Information / offences:

1. Sexual Offences listed in [Schedule 3, Sexual Offences Act 2003](#).

<sup>2</sup> See Schedule 5 'Qualifying offences for purposes of Part 10 for a full list of applicable offences.

<sup>3</sup> ACPO define potentially dangerous people as "A person who is not eligible for management under MAPPA, but whose behaviour gives reasonable grounds for believing that there is a present likelihood of them committing an offence or offences that will cause serious harm."

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

2. Violent Offences specified in the Home Office for counting rules for recorded crime / National Crime Recording Standard.
3. This Group also includes specified offences that are not serious offences as defined in the Criminal Justice Act 2000. Other serious offences are recorded as Group 2 Offences on the PNLD.

These information are to be held for an **initial 10 years clear period**. If the subject is deemed to pose a high risk of harm, the information is to be retained and reviewed after a further 10 year period.

- c. **Group 3 – All Other Offences.** Information relating to individuals who are convicted, acquitted, charged, arrested, questioned or implicated for offending behaviour which does not fall within Groups 1 or 2, including all offences capable of being heard summarily. This group poses a lower risk of harm to the public and Service community. This information is to be retained for an **initial 6 year clear period**.
- d. **Group 4 – Miscellaneous.** This group includes information relating to the following:
  1. Undetected Crime.
  2. Missing Persons.
  3. Victim/Witness information.

4. Non-criminal incidents impacting on Service personnel or Service interests that are reported to the Service Police.

**Multi-Crime Material.** This encompasses material not specifically listed above but likely to contain relevant material about multiple cases and therefore necessarily retained.

1. Police Notebooks.
  - a. General Police Duties – 6 years (except where details of a Group 1 investigation are listed when the retention period is extended to 100 years).
  - b. Special Investigations Branch – 10 years (except where details of a Group 1 investigation are listed when the retention period is extended to 100 years).
2. Daily Occurrence Books (offline Units) – 10 years (except where details of a Group 1 investigation are listed when the retention period is extended to 100 years).

A table detailing these groups and the respective retention periods is covered in Service Police Information Groupings at Annex A. To identify the appropriate Service Police Information Grouping a prepared list of all offences recorded by REDCAP is included at Annex B - Listed offences against assigned Service Police Information Groupings. Where an investigating unit identifies an offence not listed they are to engage with SPCB to assign an appropriate grouping.





**3.2 First Response - Retention.** The retention of information relating to criminal activity and known and suspected offenders allows the Service Police to develop a more proactive approach to policing. By contributing to the identification of criminal patterns and threats and helping to prioritise the deployment of policing resources, information retention assists the Service Police in the prevention and detection of crime. It is however impractical and unlawful to retain every piece of information collected. Consideration must therefore be given to the types of information that needs to be retained and the implications of storing this information in various formats. In those circumstances where individual information cannot be separated, for example Service Police Notebooks, Daily Occurrence Books etc, the entire collection of information should be retained according to the most serious offence which they contain.

**3.3 Initial Actions – Retention Assessment Criteria.** All Service Police information which is necessary for policing purposes will be held by the originating unit in accordance with MPID Chapter 26, paragraph 2.1.

The review process specifies that the Service Police may retain information only for as long as it is necessary. The Retention Assessment Criteria asks a series of questions, focused on known risk factors, in an effort to draw reasonable and informed conclusions about the risk of harm presented by individuals or offenders, with emphasis placed on specific employment within HM Forces. These questions are:

- a. **Has there been any further incident of criminality?** If so the clear period has not been met and the date for review should reflect the relevant clear period from the last recorded incident.
- b. **Is there evidence of a capacity to inflict serious harm?** It may be the case that an individual has been arrested for a relatively minor offence; the details of which would not ordinarily be retained for an extended period of time. The circumstances of the offence, however, suggest that the suspected offender has high risk tendencies that need to be monitored and managed in the future. Examples of behaviour that may cause concern in this context include animal cruelty, threats to others, violence in a domestic setting, hate-based behaviour and predatory behaviour. Any incidents involving the use of weapons should also be included in this category.
- c. **Are there any concerns in relation to Children or Vulnerable Adults?** Information relating to cases which involve a child or vulnerable adult is often particularly sensitive and highly relevant in the context of vetting and barring decisions for individuals who apply to work with these groups, whether within HM Forces or civilian life. It should be noted that within the Service community, recruits and Service personnel undergoing training, Service personnel and civilians held in Service custody (MCTC, Unit detention facilities, Operational detention facilities) and Service personnel in hospital are considered vulnerable adults.
- d. **Did the behaviour involve a breach of trust?** A willingness to betray others, especially those in a position of vulnerability or

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

dependency, is an indicator of significant criminality and often defines the line between opportunistic and premeditated offending. Offences that involve a breach of trust are particularly significant in the context of employment, vetting and barring.

- e. **Is there evidence of established links or associations which might increase the risk of harm?** Although less relevant in the context of Military policing, research in the area of criminal lifestyle and associations has demonstrated a clear link between spending time with other offenders and the likelihood of re-offending. This is particularly significant in circumstances where the identified group of offenders are already deemed to pose a risk of serious harm.
- f. **Are there concerns in relation to substance misuse?** Drug and alcohol misuse can act as a trigger or catalyst for offending behaviour. Additionally, in association with other crime-related factors, it can increase the risk of harm to others. The presence of substance misuse as a risk factor in an individual's offending or alleged offending may also affect the type of behaviour that is considered relevant for the purposes of re-setting their Clear Period prior to a scheduled review.
- g. **Are there concerns that an individual's mental state might exacerbate risk?** In the context of suspected, alleged or confirmed offending behaviour, mental health problems can become offending related and contribute to an individual's capacity for inflicting harm on others.

- h. **Are there concerns regarding an individual's potential future employment within HM Forces?** Consideration must be given to Service personnel's potential future employment within HM Forces, particularly where information is available that may indicate that s/he could abuse their position.

**3.4 Qualified Response – Reviews.** The review process is a full person information review. It focuses on an individual and any information linked to them, both electronically and hard copy. SPCB are to review in accordance with the retention periods to ensure that any information held is:

- a. **Necessary.** The information held should hold some value for policing purposes. Where an individual continues to offend or is implicated in continued offending there is a clear need to hold information relating to them in order to bring them to justice and prevent them from re-offending. Where an individual has been linked to crime in the past but is not implicated in further offending, the need to retain information relating to them will be determined by the level and type of risk they pose to the community (both civilian and Service).
- b. **Adequate.** In order to justify the retention of information they should be made as complete as possible.
- c. **Accurate and Up to Date.** All information should be accurate. Information should be updated with any new information.

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

- d. **Not Excessive.** The amount and type of information held in relation to a person should be proportionate to the threat they pose to others and the community (both civilian and Service).
- e. **Data Protection Act Compliant.** Any information of personal or sensitive personal data should also comply with the principles of the Data Protection Act 1998.

All information held by the Service Police will be subject to:

- a. **An initial evaluation.** The initial stage of review of Service Police information will be conducted at the point of input and creation and is an individual Service Police Unit responsibility.
- b. **Scheduled Reviews.** A scheduled review will be undertaken at the end of the period specified by the Service Police Information Groupings. Scheduled reviews, undertaken by SPCB, will require an assessment to be conducted on the risk of harm posed by the subject of the information under review. The key points to consider in relation to the scheduled review of Service Police information are:
  - 1. All information, regardless of type or classification, will be held for a minimum of 6 years.
  - 2. There is a presumption in favour of the deletion of information unless it is necessary for a policing purpose, is not excessive, is adequate for that purpose and is up to date.

- 3. Where an individual is believed to pose a high risk of harm, information about them will be retained for a further period as specified by the review schedule ([Para 3.1](#)).
- 4. Prior to destruction all information and investigations 15 years or over are to be considered for their value to the National Archive. Guidance is available at section 46 Freedom of Information Act (FOIA). There is a presumption that all information relating to overseas Operations (including Op Banner) are of value to the National Archive. Advice in this matter can be sought through [DBS KI Records](#) - [REDACTED]
- c. **Statutory Disclosure Review.** A review may be conducted in the following circumstances:
  - 1. **Statutory Disclosure (e.g. DBS).** A review of information being disclosed as a statutory requirement is correct and relevant to the matter in question.
  - 2. **Requests for information made by other Law Enforcement Agencies.** Personal information shared with other law enforcement agencies should be reviewed for their accuracy, adequacy and necessity.
  - 3. **Freedom of Information Act.** FOIA requests are to be reviewed. Disclosure is to be made of all the information available at the time of the request and information is only to be updated or disposed of once the request has been responded to. It is imperative that information is disclosed

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

for FOIA requests in the exact state it was stored, accurate or not.

4. **Subject Access Requests (SAR).** Under the Data Protection Act, a subject can request access to the information held about them by an organisation. When conducting a SAR, there might be a requirement to conduct a review. Again the response should reflect the information held prior to the review.

A Statutory disclosure review will be carried out by appropriately trained SPCB staff in consultation with single Service Police headquarters and Service secretariats as necessary. In all instances an auditable trail, containing the rationale behind disclosure and those responsible for making the decision is to be retained for scrutiny. The Statutory Disclosure review is to ensure that inappropriate information is not disclosed to any third party about any individual.

**3.4.1 Triggered Reviews.** A trigger review is designed to consider the lawfulness and proportionality of the retention of Service Police information outside of scheduled/statutory disclosure reviews. They can be triggered by DPM (Inv), SO1 Inv, SO1 Secretariat, SO1 Legal at HQ PM(A) (or RN/RAF equivalent), the Force Incident Crime Registrar (FICR) or OC SPCB. A trigger review will always be conducted where the lawfulness and/or proportionality of the retention is challenged by an individual or organisation.

Wherever a triggered review has been activated for electronic information, the trigger review must also link across to any hard copy documentation held on the subject concerned. Any related information

that is no longer necessary for a policing purpose must be disposed of. Any information that is found to be inaccurate must be updated. In the event that a record is inaccurate beyond alteration it must be disposed of. There is a significant difference between information that was once correct and inaccurate information that were never correct. Any personal information that is more than 10 years old (Group 2) or six years old (Group 3) and are triggered for a review should be risk assessed. If it is concluded that the subject in question continues to pose a high risk of harm, the information should be retained and reviewed again at intervals specified in the review schedule (Section 3.1).

**3.4.2 Trigger Review Panel.** All trigger reviews will, in the first instance, be prepared and considered by the SPCB Information Data Manager, who will make a recommendation to the trigger review panel if asked in relation to the information held. Contentious<sup>4</sup> cases under the Statutory Disclosure review process will also be referred. The trigger review panel will consist of:

SO1 Investigations (Chair)  
SO1 Legal  
SO1 Policy

Material relating to Royal Navy Police or Royal Air Force Police will be referred, by OC SPCB to the respective Provost Marshal's office for consideration.

---

<sup>4</sup> This is intentionally given a wide meaning but will include those issues likely to have ministerial or media interest.

The trigger review panel will decide what information should be deleted or retained. Records of decisions for all three Services are to be retained on file at SPCB for audit and examination. Challenges to this panel's decision can be made by an individual to the relevant Service PM direct.

**3.4.3 Documenting the Review Process.** The Service Police Retention Assessment Proforma ([Annex C](#)) has been designed in a table format to assist the Service Police with the requirement to record reviews and any subsequent decisions to retain information. When conducting a review of these types, if the format of a person record or the system it is held on does not allow for an automatic record of its review to be made the Service Police Retention Assessment Proforma should be completed. It should then be stored either electronically or in hard copy on the relevant file. Any system generated (REDCAP) information created to document a review must show the date of review, the reviewers name, the outcome and the reason for the decision taken. In complex cases where the review process takes several days, a time period should be recorded as the date of review. In the case of triggered reviews, the SPCB reviewing officer must provide an explanation of how and why the triggered review came about. The retention assessment criteria section of the form will determine whether or not the information under review should be retained or disposed of. This section must be used for all scheduled reviews and any triggered reviews of information that have been held for six years or more. The reviewing officer must include an explanation as to how the individual in question meets the outlined risk criteria. It is not necessary to explain how or why an individual does not meet the risk criteria if this is the case. Where a system generated (REDCAP) record is not created to document a review and the

reviewing officer is relying on the Service Police retention assessment Proforma, the outcome of review section must always be completed. It must also include an explanation of any amendments made to a record as a result of the review process.

**3.4.4 Authorising the Review Process.** All reviews that result in a decision to dispose of a record or change its category are to be prepared by the reviewing officer and approved by the authorising officer. Both appointments are found from within the Review and Retention Team at SPCB. Those reviews deemed contentious by the authorising officer will be deferred to the relevant Provost Marshal's office for a decision. Time-based disposal of Group 2, 3 and 4 information do not require any further authorisation beyond that already given.

**3.4.5 Inspections and Audits of Reviews.** To ensure the quality of review processes, inspections and audits of the reviews are to be carried out during Policing Performance Inspections.

**3.4.6 Disposal.** For the purpose of this Chapter, disposal is classed as the removal of information from all Service Police systems, justified through the review process, to the extent that it cannot be restored. Information is disposed of and removed from all Police Systems (Hard Copy and Electronic versions) because it can no longer be lawfully retained due to it being inaccurate beyond alteration, excessive or no longer necessary for policing purposes. It is, therefore essential that detail of a record disposed does not continue to exist on any Service Police systems, including paper. Where a scheduled review has taken place after a designated Clear Period and the review identifies that the subject no longer continues to pose a risk of harm, the record under



~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

review must be disposed of. Prior to destruction, confirmation will be sought from SPCB that the investigation file can be reviewed as they have reached the annotated date. Any reviews will then be conducted and on completion TNT will be given the authority to destroy. Destruction of the material will be by shredding. Material not capable of shredding will be crushed. Following shredding or crushing, the waste will be disposed of by the usual means employed by TNT. It is the responsibility of TNT to ensure that no material is disposed of from the repository until reasonable steps have been taken to ensure that any unauthorised persons cannot access the material. In accordance with the Service Level Agreement with TNT, following the disposal date occurring, TNT Staff will destroy the investigation file and all material within it. Following destruction the TNT Business Form relating to the investigation file will be returned to SPCB to ensure both SPCB and TNT have a record of the destruction for audit.

## Compliance & Qualification

**4.1 Qualification.** No Qualification Issues exist at this present time in relation to this Chapter.

**4.2 Recusal.** Policy and Guidance for Recusal, when a conflict of interest is identified, are contained within [Policy Note 04/11](#).

## References

**5.1 Legal.** The following are Legal References contained within this Chapter.

- a. [The Human Rights Act 1998](#). The Human Rights Act 1998 (HRA) incorporated most of the European Convention on Human Rights (ECHR) into UK Law. The ECHR contains fundamental rights which have a bearing on the management of police information. Specifically Article 8 protects an individual's right to respect for privacy and family life. This right is not absolute; but it may not be interfered with except in accordance with the law; in pursuit of a legitimate aim; and where it is necessary in a democratic society. This places a responsibility on the Service Police to establish a 'policing purpose' for the retention of personal information. Proportionality is also important to the management of Police information. In essence, the greater the interference with an individual's privacy, the higher the threshold required. This test is particularly relevant to the collection of information by covert or intrusive means – activity which is regulated by the [Regulation of Investigatory Powers Act 2000](#) (RIPA). The decision to retain personal information should be proportional to the person's risk of offending and the risk of harm they cause to others, and the Service and Civil community. Case law places a heavy responsibility on the Service Police to ensure that personal information is not routinely shared outside of the Service Police without a separate proportionality test being undertaken. The fact that information is retained for a policing purpose does not mean that it can necessarily be shared outside of the Service Police and/or wider law enforcement community.

~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

- b. Data Protection Act 1998 (DPA 98). Service Police information relating to an individual can be held lawfully by the Service Police providing that its continued retention can be justified for a policing purpose. Personal data is defined by the DPA 98 as information about a living person who can be identified from that data. The DPA 98 requires personal information to comply with the eight data protection principles, which are that information is:

1. Being fairly and lawfully processed.
2. Being processed for specified and lawful purposes and not in any manner incompatible with those purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary up to date.
5. Not being kept for longer than necessary.
6. Being processed in accordance with individual rights.
7. Secure.
8. Not to be transferred to countries outside the EU (or European Economic Area countries that have a bilateral agreement with the UK) without adequate protection.

The DPA 98 also requires that the subject of information can have access to it at their request. There are a number of

exceptions from the DPA 98 including Section 28 (National Security), Section 33 (Research and Statistics) and Section 35 (Legal Proceedings).

Section 29 of the DPA 98 is particularly relevant to Service Police information, because it creates exemptions to certain data protection principles where data is processed or shared for the purposes of:

1. Prevention or detection of crime.
2. Apprehension or prosecution of offenders.
3. Assessment or collection of any tax or duty.

- c. Criminal Procedure and Investigations Act 1996 (CPIA 96).

CPIA 96 has established the requirements for retaining information relevant to investigations for set periods of time. These retention periods, however, are a minimum requirement to meet the specific aim of the CPIA 96. Information should be retained for as long as it is necessary and proportionate to do so irrespective of the CPIA 96 requirements. For example, the PNC will hold conviction data until the subject of the record has reached 100 years of age regardless of how long the information is required for CPIA 96 purposes. CPIA 96 states that relevant information must be retained at least until:

1. A decision is taken whether to institute proceedings against a person for an offence.



~~OFFICIAL~~

~~Handling Instruction: Limited Circulation~~

2. The accused is convicted, acquitted or the prosecutor decides to proceed with the case.
  3. The convicted person is released from custody (or hospital) in those cases where a custodial sentence (or hospital order) is imposed.
  4. Six months from the date of conviction in all other cases.
- d. Freedom of Information Act 2000 (FOIA). The FOIA encourages accurate record keeping. A request under the FOIA does not mean that information cannot be updated once the information has been disclosed. Section 77 of the FOIA makes it an offence to deliberately alter or erase information once an application for access to them has been made in an effort to avoid having to disclose them. This means that the Service Police may have to disclose information that they hold, even if these information are inaccurate, excessive or otherwise contravene the DPA 98. It is therefore imperative that all information are reviewed for necessity and adequacy so that they can be confidently disclosed if required. A code of practice, issued under section 46 of the FOIA, gives guidance on good practice in information management. It applies to all authorities subject to the Public Information Act 1958, of which the MoD is one, or to the Public Information Act (Northern Ireland) 1923. It also contains guidance on the review and transfer of public information to an archives office for permanent preservation.
- e. Criminal Justice Act 2003.
- f. Schedule 2, JSP 830, Manual of Service Law.
- g. Schedule 3, Sexual Offences Act 2003.
- h. Criminal Justice and Court Services Act 2000.
- i. Annex B to Vol 1, Ch 6, JSP 830 Manual of Service Law.
- 5.2 Associated Policies.** The following documentation should also be read in connection with the Management of Service Police Information:
- 5.2.1** Annex A – Service Police Information Grouping.
- 5.2.2** Annex B – Listed Offences Against Assigned Service Police Information Groupings.
- 5.2.3** Annex C - Service Police Retention Assessment Proforma.
- 5.2.4** NPIA Guidance on The Management of Police Information 2010.
- 5.2.5** JSP 441 – Defence Information Management Policy and Procedures.
- 5.2.6** MPID Chapter 27 – Evidential Property.

## Training

**6.1 Training Issues.** There are no specific Training implications in relation to this chapter, however each Unit should consider the employment of suitable personnel, in order to ensure Unit archiving is managed appropriately. Continuity in employment is deemed most effective.

## Financial

**7.1 Budget Implications.** Engagement with any external agencies or Subject Matter Experts that may incur financial costs are to be cleared and authorised via SO2B, Inv & Pol, HQ PM(A). Authority out of hours can be given by an RMP officer not below Field rank but must be justified and notified to SO2B Inv & Pol, HQ PM(A) the next working day.

## Lessons Learnt

**8.1 Abridged Learning Account.** In line with MoD policy, there may be an occasion for units to produce Learning Accounts to be submitted to HQ PM(A). All considerations relevant to investigations and policing practice will be collated by way of an Abridged Learning Account, maintained by WO Inv Stds within HQ PM(A) Inv and Pol. Those which have a specific bearing on this MPID chapter can be found below.

~~OFFICIAL~~  
~~Handling Instruction: Limited Circulation~~

**Lessons Learnt – MPID 45 – The Management of Service Police Information**

Serial:	Date:	Issue:	Lesson Learnt: