NPIA
National Policing Improvement Agency
PRACTICE IMPROVEMENT

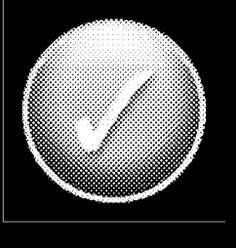
To help with fast navigation, this document contains interactive links.

- Clicking on any of the items in the main list of Contents of the document will take you directly to the section listed.

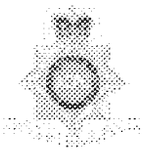
- Then, as appropriate, click on any item in the list of Contents at the start of each section for redirection to a specific subsection or item as listed.

- For immediate access to cross-referrals within the document, and any external web links, click on those items appearing in **bold** where you see the 'hand-pointer' when running over the text.

- To return to the main list of Contents, click on the base of any page in the document.



Now, click the button to go to the next page.



Guidance on

THE MANAGEMENT OF POLICE INFORMATION

Second Edition

2010

Produced on behalf of The Association of Chief Police Officers
by the National Policing Improvement Agency

This guidance contains information to assist policing in England, Wales and Northern Ireland. It is not protectively marked under the Government Protective Marking Scheme.

This guidance has been produced by the National Policing Improvement Agency (NPIA) on behalf of the Association of Chief Police Officers (ACPO). It will be updated according to legislative and policy changes and re-released as required.

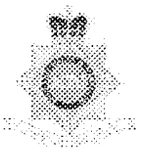
The NPIA was established by the Police and Justice Act 2006. As part of its remit the NPIA is required to develop policing doctrine, including guidance, in consultation with ACPO, the Home Office and the Police Service. Guidance produced by the NPIA should be used by chief officers to shape police responses to ensure that the general public experience consistent levels of service. The implementation of all guidance will require operational choices to be made at local level in order to achieve the appropriate police response.

If you would like to receive this publication in an alternative format, please contact:

Specialist Operations Centre
Wyboston Lakes, Great North Road
Wyboston, Bedfordshire MK44 3BY

Telephone: 0845 000 5463
Email: soc@npia.pnn.police.uk

All other enquiries relating to this publication should also be addressed to the Specialist Operations Centre at the above address.



NPIA
Notional Policing Improvement Agency

PRACTICE IMPROVEMENT

Guidance on THE MANAGEMENT OF POLICE INFORMATION Second Edition

2010

Produced on behalf of the Association of Chief Police Officers
by the National Policing Improvement Agency

First published 2006
National Centre for Policing Excellence (NCPE)/Centrex
This edition published 2010
National Policing Improvement Agency
10-18 Victoria Street
London SW1H 0NN

The National Policing Improvement Agency (NPIA) is committed to making a valuable contribution to improving public safety. ACPO and the NPIA would like to express their thanks to all those involved in the drafting of this document. All of the responses during the consultation phase of this project were appreciated and contributed to the final document.

Contents

Foreword

The purpose of the Police Service is to uphold the law fairly and firmly; to prevent crime; to pursue and bring to justice those who break the law; to keep the Queen's Peace; to protect, help and reassure the community; and to be seen to do all this with integrity, common sense and sound judgement.

Police Service Statement of Common Values

For the Police Service to be intelligence led in protecting the public, preventing crime and bringing criminals to justice then the effective management of information is vital. Since 2006 the MoPI programme has put a framework in place to improve the way forces collect, record, evaluate, review and then, most importantly, improve the quality of actions taken as a result of better quality information. The first stages of this programme are coming to an end and the improvements MoPI has made to information management and use are clear.

Forces are now making themselves ready for the introduction of the Police National Database which will revolutionise policing. If the maximum benefits are to be obtained from the PND then MoPI must continue to be at the heart of our work.

This second edition of the MoPI guidance was produced as a direct result of the experience of forces and reflects nationwide learning and experience. It emphasises the need for common standards while taking into account differing local priorities. This new guidance will ensure that forces are ready to maximise the public protection, investigation and prosecution opportunities that the PND will bring and so ensure we provide all of our communities with the best possible Police Service.

Ailsa Beaton
Head of ACPO Information Management

Preface

The murder of Holly Wells and Jessica Chapman in August 2002 by Ian Huntley, and the subsequent inquiry by Sir Michael Bichard, had a profound and far-reaching effect on the way the Police Service gathers, manages, uses and shares information. In July 2005, as a direct result of the Bichard inquiry, the Home Secretary issued a statutory ***Code of Practice on the Management of Police Information,*** hereafter referred to as the ***MoPI Code of Practice.***

As part of a wide-ranging programme of work to address the issues identified by Sir Michael Bichard, ***ACPO (2006) Guidance on the Management of Police Information*** was published. It formed the basis of a national implementation project that will run until December 2010. This revised edition of the guidance is intended to take account of the experience of implementation, as well as significant developments to the context of police information management in the last three years.

This guidance has been developed by the National Policing Improvement Agency (NPIA) on behalf of the Association of Chief Police Officers and the Home Office. The development of this guidance has involved Police Service consultation with chief officers, subject experts and practitioners. There has also been extensive contact with experts on information management from outside the Police Service.

This is not a fundamental overhaul of the existing MoPI framework, and the structure and tone of the guidance remain consistent with the previous version. That framework, encompassing a statutory code of practice under the Police Act 1996, setting out the **principles** of information management, accompanying guidance describing the **process** for information management, and associated learning and implementation products, has repeatedly been tested and found to be fit for purpose. In this guidance the abbreviation MoPI will be used to refer to the national framework for the management of police information in its entirety.

There have been no changes to the statutory *Code of Practice on the Management of Police Information.* This guidance describes the processes that support the principles set out in the ***MoPI Code of Practice.*** It is designed to provide a common national framework for the management of police information, highlighting the importance of common standards in high-risk areas of activity. ***ACPO (2010) Guidance on the Management of Police Information,* Second Edition** hereafter referred to as the ***MoPI Guidance,*** is designed to contribute to enhanced public safety by improving the ability of the Police Service to properly manage and share operational information within a consistent framework as required by the Bichard recommendations.

The Police Service has never been under greater public scrutiny in relation to how it gathers, manages and uses information about individuals. Similarly, the balance between an individual's human rights, civil liberties and public protection has never been so closely examined. The recent European Court of Human Rights judgment in the case of *S and Marper v The UK* [2008] ECHR 1581 on the lawfulness of retaining DNA samples of unconvicted individuals has potentially wide-ranging implications, as does the broader public policy debate about the extent to which the UK has become a 'surveillance society'. It is, therefore, important that the management of police information (MoPI) is seen to apply equally to information held nationally and locally.

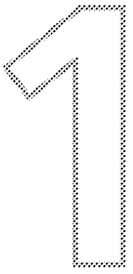
MoPI is a framework; it does not prescribe how all information should be dealt with on a case-by-case basis. Chief officers are accountable in law for those decisions and nothing within the ***MoPI Code of Practice*** or the ***MoPI Guidance*** changes that accountability. However, the principles of MoPI provide a way of balancing proportionality and necessity that are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information. The ***MoPI Code of Practice*** and the ***MoPI Guidance*** are components of a nationally agreed implementation strategy. This strategy involves the definition of threshold standards drawn from the ***MoPI Code of Practice*** and the ***MoPI Guidance.*** These standards are part of the overall package that chief officers should have regard to under the terms of the Police Act 1996.

The ***MoPI Guidance*** is designed to contribute to enhanced public safety by improving the ability of the Police Service to properly manage and share operational information within a nationally consistent framework. ACPO recognises that chief officers are required to balance resources against local policing needs. Each chief officer is afforded the flexibility to decide on the scale of implementation for each standard contained within the the ***MoPI Guidance,*** based on the individual structure, resources, priority, risk and the local needs of each force.

The ongoing development, under the IMPACT programme, of the Police National Database (PND) provides an example of the requirement for a common and consistent approach to the management of information across the Police Service. The benefits of the PND, in terms of the identification of links between people, objects, locations and events across different force areas, depend on

the adoption of a consistent approach. This guidance is not, however, technical in nature, and does not describe the functions or operations of any particular information management system. Guidance on the PND will be issued prior to its going live.

There is a need for MoPI development and planning to continue as a dynamic process beyond initial implementation. Forces should keep policies and procedures under regular review to ensure effectiveness, efficiency and continued alignment with MoPI principles.



The Purpose of Managing Police Information

This section describes what is meant by police information and why it is vital for the Police Service. It also provides an outline of the legal basis for the management of police information and the stages involved in it.

Key principles of this section are that:

- **This guidance is derived from *ACPO (2005) Code of Practice on the Management of Police Information;***
- **Police information is information for a policing purpose;**
- **Police information must be managed lawfully;**
- **Information is a corporate resource for the Police Service.**

Contents

1.1 What Is this Guidance?

Effective policing depends on efficient information management and this guidance sets out a framework for the management of police information. As such, the guidance is based on work over many years on defining policing processes and developing national standards. This guidance brings together this work in a coherent national framework for the management of police information. In so doing, it meets key recommendations of the Bichard Inquiry that called for the development and implementation of a statutory Code of Practice for police information management.

This guidance supports ***ACPO (2005) Code of Practice on the Management of Police Information,*** Appendix 1, (referred to in this guidance as the ***MoPI Code of Practice***).

The ***MoPI Guidance*** replaces the following:

- ***ACPO (2004) Code of Practice on Data Protection;***
- ***ACPO and HMCE (1999) Code of Practice on the Recording and Dissemination of Intelligence Material;***
- ***ACPO and HMCE (1999) Standards for the Recording and Dissemination of Intelligence Material;***
- ***ACPO (2006) Guidance on the Management of Police Information.***

All other guidance relevant to the management of police information remains valid. Specific links to other guidance are indicated in the text.

1.2 What Is Police Information?

For the purposes of this guidance, police information is information required for a policing purpose. The ***MoPI Code of Practice*** 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 police arising from common or statute law.

These five policing purposes provide the legal basis for collecting, recording, evaluating, sharing and retaining police information. The policing purposes set out in the ***MoPI Code of Practice*** do not replace or supersede any existing duty or power defined by statute or common law.

It is essential that a policing purpose is established in order for information to be legally held.

The policing purposes set out in the ***MoPI Code of Practice*** are deliberately defined at a high level and do not define every policing activity in detail. The fact that individual activities are not listed does not mean that there is no legal basis for performing the activities. For example, information relating to key policing functions such as roads policing, public order, counter-terrorism or protection of children and other vulnerable groups, while not specifically referred to, will fit within one or more of the policing purposes.

The five policing purposes are not mutually exclusive. Information can be collected for one policing purpose and used for another.

Policing relies on continuous risk management. It is essential that processes for managing police information focus on managing the risk attached to that information. This can be done by ensuring that there are clear and consistent processes for collecting, recording and evaluating information, and by establishing effective processes for taking appropriate action on the basis of police information. Later sections of this guidance discuss this in more depth, but effective intelligence management is at the heart of police information management.

Intelligence management involves linking information from a wide range of sources in order to build up a composite picture. It aims to highlight links between people, objects, locations and events that are essential in supporting the policing purposes previously described. Identifying links enables decisions to be made about priorities and resources needed to manage risk. The decision-making process is described in detail in the National Intelligence Model (NIM).

NIM depends on information to feed the intelligence process. The implications of this on the way in which information is managed are described in **2 The Process for Managing Police Information** and ***ACPO (2005) Guidance on the National Intelligence Model.***

1.3 Information as a Resource for Policing?

Collection of appropriate information, its accurate assessment and timely analysis, is vital to effective and efficient policing.

Information collected for one policing purpose may have a value to another; therefore, all police information should be treated as a corporate resource. Information collected for one business area within a force may be relevant elsewhere in the force, or to another force or agency.

It is essential that information can be collected, recorded and evaluated in a consistent manner across organisational and force boundaries. Police information is a corporate resource for the whole Police Service; it should not matter where the information originated from and should be available to support all policing purposes across the country.

Information has, historically, been held in business areas and IT systems that are neither connected nor searchable. This has meant that, even within the same force, it has been difficult to link people, objects, locations and events. This situation is exacerbated at a regional and national level because of a lack of common standards for information recording and evaluation. As a result, sharing information within the Police Service and with key partners is unnecessarily complex. The process for ensuring that police information is a corporate resource at both force and national level is described in **2 The Process for Managing Police Information.**

This guidance provides a definition of national standards for police information management to support the establishment of a common information infrastructure for policing. The IMPACT programme is developing a national capability for the Police Service to link people, objects, locations and events across force boundaries to provide a national information resource. That programme is underpinned by this guidance.

For further information on the IMPACT programme, see **http://www.npiaextranet.pnn.police.uk/microsite/impact/index.html**

1.4 Legal Basis for Managing Police Information

In order for police information to be made available to support policing purposes the legal framework should first be understood. This guidance highlights the key principles that should be satisfied for police information to be managed lawfully; it does not set out the legal framework in detail. It should be emphasised that compliance with the law can never be ignored because it is inconvenient.

There are a number of stages to achieving lawful management of police information. These stages are summarised below and apply to all the phases of the information management cycle that are described in detail in this guidance.

Establishing a policing purpose

Establishing a policing purpose is the cornerstone of effective management of 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**.

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. The HRA requires UK legislation to be compatible with the ECHR and makes it unlawful for a public authority, including a police force, to act in a way that is incompatible with rights defined by the ECHR.

The ECHR sets out a framework of fundamental rights, including the right to life (Article 2) and the right not to be subjected to torture, inhuman or degrading treatment (Article 3). Article 8 of the ECHR 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 police forces to establish a policing purpose for collecting, recording and retaining 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).

Further guidance on the HRA can be found at:
http://www.justice.gov.uk/guidance/humanrights.htm

Is police information personal data?

Once the policing purpose is established, the issue arises of whether the information is covered by the Data Protection Act 1998 (DPA). If the information is personal or sensitive personal data then, under the terms of the DPA, it must be managed in accordance with the eight data protection principles.

Personal data is defined by the DPA as information about a living person who can be identified from that data. Much police information is covered by the DPA, and is referred to in this guidance as personal information.

What are the requirements of the Data Protection Act 1998?

The DPA requires personal information to comply with the eight data protection principles which are that information is:

- Being fairly and lawfully processed;
- Being processed for specified and lawful purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate and, where necessary, up to date;
- Not being kept for longer than is necessary;
- Being processed in accordance with individual rights;
- Secure;
- 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.

It is important to bear in mind that the application of the DPA 1998 depends on circumstances. As such, there is a burden of responsibility to audit personal information of a sensitive nature. For example, information showing an individual in a public place taken from an overt CCTV system may be personal information under the terms of the DPA, but is far less sensitive than a picture of an individual in their bedroom obtained from a covert device deployed with the appropriate RIPA authorities. In discharging responsibilities under the DPA there must be regard to the principle of proportionality; in short the more sensitive the information, the higher the threshold for processing.

The DPA also requires that the subject of information can have access to it at their request. There are a number of exemptions from the DPA including section 28 (national security), section 33 (research and statistics) and section 35 (legal proceedings).

Section 29 of the DPA 1998 is particularly relevant to police information because it 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.

The exemptions apply to certain principles of the DPA where the application of those principles would be 'likely to prejudice' the purposes referred to above. These exemptions should be applied on a case-by-case basis and cannot be used to justify routine data processing. Further information on the DPA is available at **http://www.ico.gov.uk** and ***ACPO (2009) Manual of Guidance on Data Protection***.

1.5 Stages of Managing Police Information

There are a number of stages in the management of police information:

- Collection;
- Recording;
- Evaluation and Actioning;
- Sharing;
- Review, Retention and Disposal.

These stages are described in detail in subsequent sections.

2

The Process for Managing Police Information

This section describes the need for corporate and consistent processes to manage police information, and the implications for the way in which police information is managed within forces.

Key principles of this section are that:

- **It is essential to have common processes for managing police information across the Police Service.**
- **Certain police information will have a particular significance for policing purposes.**
- **There needs to be a link between police information that is held in different business areas. This should be managed through an information management strategy.**
- **There are a number of core responsibilities for managing police information that should be in place in every force.**

Contents

2.1 Need for Common Processes

Policing purposes require information to be collected on a wide range of activities. This information will come from various sources and will be received in different ways. As a result, information collected for one policing purpose may need to be related to information collected elsewhere and for a different purpose. This requires consistent processes to be in place across all policing activities in order to manage police information as a corporate resource for the Police Service as a whole.

At force level there is a need for processes to be in place enabling information to be linked and composite records to be maintained. Forces should have the ability to have central oversight of all information held within their organisation. This can be facilitated by technology, although even the best IT systems are dependant on consistent processes being in place and adhered to. This guidance does not specify any technological solutions for information management, but sets out common business processes for managing police information.

2.2 Records Management

The management of records is fundamental to effective information management. The integrity of police information relies on the information being trusted, acceptable, useable and available. To assist the evaluation, actioning, sharing and review of information, the information should be in a format that is accessible and easy to use, whether it is an electronic, photographic or paper record.

The purpose of records management is to ensure that police information is documented and maintained in such a way that its evidential weight and integrity is not compromised over time. To achieve this, records need to be managed throughout their lifecycle from creation to disposal. This process involves the audit and maintenance of records to enable them to remain useful for a policing purpose. This also enables the discharge of legal responsibilities outlined in **1 The Purpose of Managing Police Information.**

Records should be managed in line with a records management policy. For further information see ***Lord Chancellor's (2002) Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000.***

2.3 Critical Information Areas

Some police information will be particularly valuable to policing. This guidance cannot describe exactly what police information will be critical in any given circumstance; decisions can only be made by staff in possession of the relevant facts.

The National Intelligence Model (NIM) has a significant bearing on determining critical police information. The development of a National Strategic Assessment, which identifies overall risk areas for policing, informs the National Community Safety Plan. The strategic assessments made at force and BCU level are used to set a control strategy defining particular priorities. The control strategy should form the basis of an intelligence requirement that identifies specific information needs, depending on local circumstances. There is certain information, however, that should always be considered:

- Information about known or suspected offenders;
- Information obtained from sensitive or covert sources;
- Information about serious offending, including
  - terrorism
  - serious and organised crime
  - serious sexual and violent offending
  - offences against children and vulnerable adults
  - domestic violence offences
  - series offending linked to persistent and prolific offenders;
- Information about threats to life or of serious harm.

Information on these critical areas will comprise factual information such as details of arrests, charges and statements, as well as details of suspected offending or the method employed to commit offences (modus operandi or MO).

Further information on this process can be found in ***ACPO (2005) Guidance on the National Intelligence Model.***

In discharging responsibilities for the management of police information, chief officers should have regard to their duty to protect the public, particularly those members of society such as vulnerable adults and children who are less able than others to protect themselves. This is reinforced by the Human Rights Act 1998 (HRA), particularly Article 2 (right to life) and Article 3 (prohibition of torture, inhuman or degrading treatment). Case law has stressed the responsibilities of the police to ensure that these rights are safeguarded. Forces should, therefore, should have specific arrangements in place to manage information relating to public protection.

The ***MoPI Code of Practice*** acknowledges that there are classes of information which are critical to efficient public protection arrangements, described as 'certain public protection matters'. Such matters are a subset of public protection generally and refer to only those offenders who pose the highest possible risk of harm.

For the purpose of this guidance, **'certain public protection matters'** are defined as:

- Information relating to all offenders who have ever been managed under Multi-Agency Public Protection Arrangements (MAPPA);
- Information relating to individuals who have been convicted, acquitted, arrested, questioned, charged or implicated in relation to murder, a serious offence as specified in the Criminal Justice Act 2003, or historical offences that would be charged as such if committed today;
- Potentially Dangerous People – those who have not been convicted of, or cautioned for, any offence of a sexual or violent nature and who do not fall within any of the MAPPA categories. Their behaviour, however, gives reasonable grounds for believing that there is a real likelihood of them committing an offence or offences likely to cause serious harm. For further information see ***ACPO (2007) Guidance on Protecting the Public: Managing Sexual Offenders and Violent Offenders***.

For further information on reviewing and retaining information related to certain public protection matters, see **7 Review, Retention and Disposal.**

2.4 Business Areas for Managing Information

Police information will be recorded in a number of locations, depending on the specific purpose for which it has been collected, for example, records of detainees will be held in a custody system. It is important, however, that a record stored in one business area can be linked to a record in another one.

There are a number of business areas holding police information that contain records that are particularly significant for policing purposes. These include:

- Crime Recording;
- Domestic Violence;
- Child Abuse Investigation;
- Public Protection;

- Missing Persons;
- Case and Custody;
- Incident Records;
- Firearms Licensing;
- Intelligence.

Business areas containing sensitive information:

- PNC;
- ViSOR;
- PND.

These various business areas have distinct criteria for how information is recorded on them, such as the National Crime Recording Standard, but these standards should support the fundamental principle that information held in any business area is capable of being readily linked with information held in any other police business area.

2.5 Information Management Strategy

The previous subsections established the need for information to be managed corporately and for critical information to be captured for a policing purpose.

In order to facilitate this, the processes for managing police information within each force should first be defined in a force Information Management Strategy (IMS) and further details contained in supporting policy or procedure documentation. The ***MoPI Code of Practice*** requires an IMS to be developed within each force and maintained under the responsibility of a chief officer.

The IMS is a high-level document which sets out the principles applying to information management within the force. The strategy will be owned by chief officers and available to all staff to review. It should also be made available to partners and the public.

The IMS identifies the information community within the force and defines the processes for managing information within the force and with partners. It allows information to be exploited wherever it is needed within the force, and defines how barriers can be overcome.

The IMS sets out the following:

- Who is responsible for police information held within the force;
- The purposes for collecting and holding information;
- Which business areas hold information within the force, and the standards that will apply within those areas;

- The safeguards applied to police information held by the force;
- The relationship between police information held within different business areas;
- Which processes ensure that police information is audited for accuracy and relevance to the policing purposes;
- What controls are applied to ensure the integrity and security of police information held by the force;
- The training in place to support the management of police information;
- The dedicated resources in place to support the delivery of the IMS and their relationship to other business areas;
- Arrangements for receiving records and monitoring record keeping;
- How the force complies with national and local security policy and standards.

2.6 Responsibilities

The processes involved in the management of police information are varied and complex. Subsequent sections of this guidance define specific responsibilities relating to the collection, recording, evaluation, actioning, sharing, review, retention and disposal of police information.

There are a number of core responsibilities which should be in place centrally in order to support effective information management. This subsection defines those responsibilities. They should not be seen as additional requirements on forces to those required by the NIM. These responsibilities are complementary to those outlined in the people assets in ***ACPO (2005) Guidance on the National Intelligence Model.*** Existing role profiles may be adapted to include the responsibilities required for managing police information.

The most suitable staffing and structural arrangements will vary between forces depending on size, resources and operational responsibilities. The core responsibilities should be clearly outlined in the IMS.

2.6.1 Chief Officer

The chief officer has overall responsibility for a force's compliance with the ***MoPI Code of Practice*** and the implementation of this guidance. The chief officer owns the IMS and has responsibility for ensuring that force policies and processes comply with this guidance.

In discharging these responsibilities, chief officers may wish to ensure that there is a central oversight role for all information held by the force. Such a role would be accountable to the chief officer for the everyday management of police information within the force.

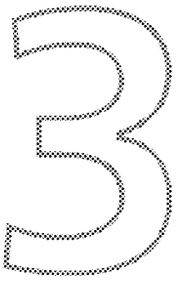
A number of forces have already followed good practice by appointing a chief information officer at senior management level to oversee information management within the organisation.

Alongside the requirements of the ***MoPI Code of Practice,*** the Data Protection Act 1998 places a legal obligation on the chief officer, as data controller, to comply with the data protection principles, subject to exemptions, in relation to all personal information controlled by the force.

2.6.2 All Staff

All police staff involved in the management of police information have the following responsibilities:

- Apply the basic principles of effective information management as contained within the ***MoPI Code of Practice*** and this guidance;
- Apply data quality principles to all police information as set out in **4 Recording of Police Information;**
- Apply operating rules relevant to the business areas to which they have access;
- Apply rules relating to information security;
- Ensure compliance with all relevant legislation including the Human Rights Act 1998, Data Protection Act 1998 and Freedom of Information Act 2000.



Collection of Police Information

This section explains why police information is collected, and how it is collected.

Key principles of this section are:

- **Police information is collected for a policing purpose;**
- **Police information is collected in line with requirements defined by the NIM process;**
- **Collection is the first stage in the management of police information;**
- **Information is collected in one of three ways – through routine collection, tasked information and volunteered information.**

Contents

3.1 Why Police Information Is Collected

The collection and recording of police information is vital to effective policing.

The collection of police information is the start of the information management process; therefore, when information is collected it is essential that it is processed accurately and consistently. This stage should not be seen in isolation as it affects all other stages of information management, from how the information is recorded to how long it will be retained.

The principles and standards of police information management should apply from the point of collection. A force Information Management Strategy (IMS) allows for information requirements to be set and, therefore, determines what information should be collected. The IMS supports the setting of force and BCU level intelligence requirements, as a dynamic process, in accordance with NIM. These requirements support service delivery and determine business needs through identified national and force/local policing plans.

Police information is collected, evaluated, analysed and risk assessed for appropriate action. This includes evaluation for its intelligence value as well as its being used for business management and statistical analysis. The collection and subsequent recording and evaluation of police information allow areas of risk to policing business to be identified, prioritised and actioned.

The means of collection of information is relevant to how the information should be processed. For example, there is a distinction between information that is volunteered, such as the data in a crime report, and that which is gathered covertly, for example, from a covert human intelligence source. In some circumstances the way in which police information is collected may lead to specific requirements as to its recording and use, for example, information covered by the Regulation of Investigatory Powers Act 1998 (RIPA).

3.2 How Police Information Is Collected

Police information is collected in a number of ways. The focus on neighbourhood policing has seen an increase in the volume of volunteered information relating to crime and disorder. The adoption of intelligence-led approaches to policing has resulted in an increase in information gathering through prioritised tasking and coordination processes.

Police information is collected reactively or proactively through routine collection, tasked information or volunteered information.

3.2.1 Routine Collection

This is where information is collected as part of routine operational and policing activity.

Much of this information is only relevant for the specific policing purpose for which it was collected. Some information collected as part of routine business will, however, prove to be relevant to an entirely different policing purpose.

All policing activities generate police information, for example:

- Responding to incidents;
- Arrests;
- Targeted patrol;
- Stop and account;
- Stop and search;
- Countering anti-social behaviour;
- Firearms licensing;
- Traffic stops;
- Criminal investigations;
- Public inquiries;
- CCTV;
- Automatic Number Plate Recognition (ANPR);
- Registration of sex offenders.

Standards for recording police information are covered in **4 Recording Police Information.**

3.2.2 Tasked Information

Tasked information is information which has been deliberately sought out and collected for a specific purpose. It refers to prioritised collection on problems and targets identified within intelligence requirements through the NIM tasking and co-ordination process. A tasking can be at a national, regional, force, BCU or neighbourhood level and can be either short or long term.

Tasking may be the consequence of a long-standing intelligence requirement or as a result of a specific, short-term, operational need. This will depend on whether the information is in relation to a specific issue, for example, where information is needed to identify the car a named suspect is using, or whether it is a general requirement, for example, where information is needed on the supply of Class A drugs in a specific area. Tasked information may also arise from collecting information during major crime investigations. This will usually be on a short-term basis and for a specific reason in relation to an investigation, for example, house-to-house enquiries.

Tasking information can take place as part of the normal briefing process or a daily briefing of patrol officers, or it could form a briefing as part of a planned operation using specialised resources such as surveillance teams or ANPR. The information collected from a tasking will usually be reported by attending a debrief and verbally informing the supervisor, and/or completing a 5x5x5 Information/Intelligence Report. Once the information has been disseminated at a debriefing, it will be recorded in the most appropriate format. For more information see ***ACPO (2006) Guidance on the National Briefing Model.***

Tasked information usually derives from:

- Intelligence collection plans;
- Proactive policing activity, for example, surveillance;
- Tasking of CCTV and ANPR systems;
- Tasking of covert human intelligence sources (CHIS);
- Searching of internal and external databases in response to a specific tasking, eg, telephone billing data for a major crime inquiry.

3.2.3 Volunteered Information

Volunteered information refers to any information that is received which may not have been collected as a result of being tasked or routinely collected. This type of information is usually collected from the general public, community contacts and partners.

Volunteered information may not necessarily relate to a specific tasking or intelligence requirement. It is usually received because people want something done with the information, for example, if a member of the public calls with information about a fight occurring outside a pub.

Volunteered information can also refer to information which has been asked for by the police. For example, following a police appeal for information on a Ford Transit van used in an armed robbery, a member of the public may report a sighting of the vehicle.

Community intelligence can also be regarded as volunteered information. Local information from a community is received and, when assessed, can provide intelligence on issues which affect neighbourhoods.

This voluntary method of collecting information can be received in any format at any time. It will include:

- Any public contact through command and control or crime systems;
- Voluntary organisations, for example, Neighbourhood Watch;
- Anonymous information, for example, Crimestoppers or the anti-terrorism hotline;
- Partner agencies, for example, social services for a child protection matter.

For further details on information sources, see ***ACPO (2005) Guidance on the National Intelligence Model.***

3.3 Responsibilities

3.3.1 Managers

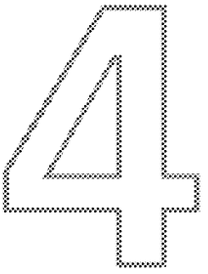
- Ensure that clear intelligence requirements have been set;
- Ensure that the control strategy drives the intelligence requirement;
- Ensure staff are made aware of what the intelligence requirements are.

3.3.2 Supervisors

- Provide briefings and taskings to staff deployed on information collection;
- Provide the opportunity for debriefing operations.

3.3.3 Users

- Ensure that they are aware of the current intelligence requirements;
- Ensure that information is collected for a policing purpose.



Recording Police Information

This section gives guidance on how and where police information should be recorded for a policing purpose. It also outlines how the method of recording police information can facilitate subsequent searching and linking to other information.

Key principles of this section are:

- **Police information is recorded for a policing purpose;**
- **Police information must be recorded correctly first time;**
- **Recorded police information should be searchable and retrievable;**
- **Police information may be recorded in different business areas depending on its purpose;**
- **Person records allow for police information held in different business areas to be interlinked.**

Contents

4.1 Why Recording Information Is Important

Recording police information allows it to become a corporate resource by transferring the information from an individual to the organisational memory.

The way in which police information is recorded allows for it to be evaluated and actioned. The benefits of recording police information in accordance with national standards include:

- Ensuring that all police information is held in accordance with the law;
- The ability for the information to support decision making through NIM;
- Providing an auditable decision-making process;
- The ability to evaluate, risk assess and corroborate other related information;
- The ability to share information within the Police Service, other agencies and the public.

Failure to record information correctly can prevent forces from being able to adequately manage risk to the public, create a potential misuse of resources and so fail to meet national and local policing objectives.

4.2 Principles of Recording

There are a number of key principles which apply to the recording of police information regardless of its format and business area where it is held. The person recording the information must ensure that they have regard to these principles.

- A record must have been created for a policing purpose.
- All records must comply with the data quality principles set out in **4.3 Data Quality Principles.**
- A record of police information is the start of an audit trail and must identify who completed the record, when it was completed and for what purpose.
- Before recording information, checks should be made in other business areas to see whether this information is already held; this will help to avoid unnecessary duplication.
- If information is recorded on an individual who is the subject of an existing record, then the record should reflect this.
- If it becomes apparent that the information being recorded is connected to other information then it must be appropriately linked.

- Police information must be recorded as soon as practicable in accordance with the standards relating to the business area in which the information is held.
- When recording police information, consideration should be given to the application of the appropriate Government Protective Marking Scheme (GPMS) marking.
- Where appropriate, the source of the information should be recorded to ensure accuracy and to assist in requests for further information.

4.3 Data Quality Principles

Data quality is fundamental to successful information management. It is essential that all information is recorded properly at the outset. Failure to do so will lead to further work and an increased likelihood of missing a vital link. High-quality information helps to ensure that appropriate action is taken, means that information can be shared where possible, and that it can be retained, reviewed and disposed of appropriately.

All police information must conform to the following data quality principles:

- **Accurate** – care must be taken when recording information and, where appropriate, the source of the information must also be recorded. If there is any doubt over the authenticity of the information, clarification must be sought from the source. Inaccurate information must be corrected as soon as possible. In ensuring accuracy it is important not to delete historic information that may be significant (such as details of previous addresses).
- **Adequate** – recorded information must be accurate and sufficient for the policing purpose for which it is processed. The nature of the event will determine the information that is relevant. All recorded information must be easily understood by others.
- **Relevant** – information recorded must be relevant to the policing purpose. Opinions need to be clearly distinguished from fact.
- **Timely** – information must be promptly recorded into the relevant business area in accordance with the agreed timescales.

4.4 How Police Information Is Recorded

Police information can be recorded in different formats and held in different business areas according to the purpose for which the information has been recorded. Police business requires information to be linked within forces and across force boundaries.

The IMS should specify where information is recorded. It is a requirement of the Data Protection Act 1998 that business areas that contain personal data are registered with the Information Commissioner. For further information see ***ACPO (2009) Manual of Guidance on Data Protection.***

4.4.1 Crime Recording

Forces use the National Crime Recording Standard (NCRS) to record crime. The NCRS promotes consistency between police forces in recording crime and a victim-orientated approach to crime recording. This standard has three basic principles:

- All reports of incidents will result in the registration of an incident report by the police (whether from victims, witnesses or third parties and whether crime related or not);
- An incident will be recorded as a crime (notifiable offence) if, on the balance of probability,
  i) the circumstances as reported amount to a crime defined by law, and
  ii) there is no credible evidence to the contrary;
- Once recorded, a crime will remain recorded unless there is additional verifiable information to disprove it.

Crime reports will record details which include:

- Name;
- Time, day, date of incident;
- Time, day, date of recording;
- How the crime was reported;
- Who reported the crime and the method;
- Location;
- Modus Operandi (MO) – it is particularly important that this field is as complete as possible because it will often form the basis for the identification of suspects.

For further guidance see ***Home Office (2009) Counting Rules for Recorded Crime*** at **http://www.homeoffice.gov.uk/rds/countrules.html**

In some instances there may be some recorded crimes which will be classified as a 'no crime', according to specific criteria. For further information see ***Home Office (2009) Counting Rules for Recorded Crime*** Section C at **http://www.homeoffice.gov.uk/rds/countrules.html**

4.4.2 Domestic Abuse

Information in cases of domestic abuse must be recorded in compliance with the NCRS. It is essential that the crime record clearly identifies the domestic abuse and includes information such as the location and identity of the person making the report, whether the parties are injured, description of the suspect, and identity of the parties involved including the victim and children. For further information see ***ACPO (2008) Guidance on Investigating Domestic Abuse.***

4.4.3 Child Abuse Investigation

There are a number of systems which contain information on child abuse investigation matters; some of these are paper based. Most systems will record information relating to referrals made to the police and social services. Information recorded should include, for example, names, allegation details and dates, details of suspects, other family members and significant people, and the initial decision made at the time of the report. As many child abuse records are categorised under the victim's details, it is particularly important that the details of suspects or offenders are clearly identified within the record to enable cross-referencing.

For further information see, ***ACPO (2009) Guidance on Investigating Child Abuse and Safeguarding Children,*** **Second Edition.**

4.4.4 Public Protection

In this guidance, public protection refers to details of offenders who have been convicted of serious sexual or violent offences and who are the subject of extended supervision or registration arrangements. Public protection also includes potentially dangerous persons who may not have been convicted of serious offences but whose behaviour causes significant concern about their risk of serious offending in the future. See **2.3 Critical Information Areas.**

The Violent Offender and Sex Offender Register (ViSOR) is a national system for managing violent and sex offenders. It is operated by the Police Service in conjunction with the National Offender Management Service. ViSOR allows information and intelligence regarding violent and dangerous offenders to be exchanged, and records information such as names, arrests, appearance, MO, pets and up-to-date images.

Public protection records generally contain sensitive information relating to victims of serious sexual or physical assault; details of the source of information in respect of the offence or incident under investigation; details of any joint agency investigation and, where relevant, information relating to the offender.

It is essential that this information is recorded accurately and is searchable against other business areas in order to ensure consistency of information. For further information refer to ***ACPO (2007) Guidance on Protecting the Public: Managing Sexual Offenders and Violent Offenders.***

4.4.5 Missing Persons

Information on missing persons should be recorded on a National Reporting Form – Missing Person Investigation. This is a nationally recognised form which has been adopted by forces, either in a paper format, or by using IT systems which comply with the information recording requirements of the form. Information to be recorded on this form includes missing status details of the missing person, informant details and circumstances leading to their disappearance. For further information see ***ACPO (2010) Guidance on the Management Recording and Investigation of Missing Persons,*** **Second Edition.**

4.4.6 Case and Custody

A custody system allows for the management of processes involved in the detention of individuals in a police custody suite. Information on these systems includes prisoners' personal details and arrest details.

A case system manages all aspects of case file preparation following the decision to instigate proceedings. This includes the management of defendants and witnesses.

There are a number of different case and custody systems within the Police Service, for example, the National Strategy for Police Information Systems (NSPIS) case and custody. These systems are designed to interface with Crown Prosecution Service systems and enable communication across all agencies in the criminal justice system.

Information recorded on these systems should meet the standards for them alongside the general data quality principles as outlined in **4.3 Data Quality Principles.**

4.4.7 Incident Records

The National Standard for Incident Recording (NSIR) ensures that all appropriate incidents, whether crime or non-crime, are recorded by the police in a consistent and accurate manner. This allows the resulting information to be used at local and national levels to meet the management and performance information needs of all stakeholders. An incident report is defined as any communication, by whatever means, from any person, about a matter that comes to police attention and which is required by the NSIR to be recorded. When recording information on an incident record, there are a number of minimum data standards to be complied with:

- Time and date when the report was received;
- Method of reporting;
- Time and date when the report was recorded;
- An incident Unique Reference Number (URN);
- Details of the person making the report (name, address and telephone number);
- Sufficient information to describe the location and nature of the report.

For further guidance see ***Home Office (current) Counting Rules*** at **http://www.homeoffice.gov.uk/rds/countrules.html**

4.4.8 Firearms Licensing

The National Firearms Licence Management System (NFLMS) holds information about legally held firearms. Information recorded on NFLMS includes:

- Data on persons holding a shotgun – name, address, date of birth, certificate number, conditions of licence, serial numbers;
- Section 1 firearm – the same details as above and also ammunition;

- Registered dealers – name, address, licence information and what explosives can be held, this information is linked to the PNC;
- Revocations and refusals.

4.4.9 Intelligence

An intelligence business area is the central information area for recording and evaluating police information that has an intelligence value. This business area usually contains a central index of the names of people who are of interest to the police. Information recorded in this business area is influenced by the intelligence requirements identified by forces.

Information for an intelligence purpose is recorded on the 5x5x5 Information/Intelligence report. The 5x5x5 is a tool which allows the Police Service to manage information which has risk attached to it. It is the standard format for managing the evaluation, source and the provenance of the information, and the manner in which it should be handled and disseminated. The use of a 5x5x5 provides an audit trail which is integral to the NIM process. It ensures consistency between forces and enables forces to share intelligence more easily. The majority of information in an intelligence business area should be recorded using the 5x5x5.

Some information that may be considered for intelligence purposes, however, will have been recorded in other business areas, eg, crime reports, custody records. In some circumstances there may be an automatic link between these areas; in other circumstances it may be necessary to manually update the intelligence business area by submission of a 5x5x5.

There should be the capability to link records held in the intelligence business area. Forces should have the ability to link information across business areas in terms of people, objects, location and events. By placing a marker against information which can be linked, it highlights that there is other information known and so allows for the appropriate action to be taken, for example, where an individual is the subject of a number of crime reports with a similar MO.

For further information see **Appendix 2.**

4.4.10 Police National Computer

The Police National Computer (PNC) contains significant police information recorded in compliance with national standards. A PNC record is created for persons who:

- Are the subject of judicial process for recordable offences, including information about their current status;
- Have previous convictions for recordable offences, including reprimands, warnings and cautions;
- Are currently disqualified from driving;
- Are wanted by the police;
- Have been arrested and fingerprints or DNA samples have been taken;
- Are missing or have otherwise come to notice;
- Have a firearms marker.

The PNC also contains links to the Driver and Vehicle Licensing Agency (DVLA) driving licence database. The vehicles application contains details of over 50 million vehicles including all vehicles registered in the British mainland, foreign vehicles that have been reported stolen in the UK and other vehicles of particular interest to the police. The PNC also contains details of certain categories of objects known as property, including specific items of contractors' plant, vehicle attachments such as trailers, engines, containers and sidecars, marine craft, animals and firearms.

Information recorded onto the PNC should adhere to the ***PNC Code of Practice 2005*** and ***PITO (2005) PNC User Manual Volumes 1 and 2.***

4.5 Person Records

Categorising records allows information to be arranged so that a force knows what information is held where. It also helps to identify the information that is needed in support of the force information management strategy and intelligence requirements.

Records can be categorised in terms of people, objects, locations and events (POLE). This guidance concentrates on person records as these are of greatest importance and present most risk for offenders, victims and sources. This approach also acknowledges the legal requirement to process personal information appropriately. Further development of the standards for records of objects, locations and events is being taken forward within the IMPACT programme.

For the purpose of this guidance, the creation of a person record will contain, as a minimum, one of the following:

- Forename;
- Family name;
- Partial name;
- Nickname;
- Alias.

A description without a name attached will not lead to the creation of a person record. Other desirable basic fields to include on a person record are:

- Age (date of birth);
- Sex;
- Colour/Ethnicity;
- Height.

In order to create a person record, every effort should be made to establish a person's identity. The greater the detail, the greater the likelihood the record will be unique. This should, however, be proportionate to the reason for recording the information, for example, more information would be needed to identify a murder suspect compared with a witness to a shoplifting.

Establishing a unique reference number (URN) which can be linked to a person record is a desirable factor in the organisation of information. Having a URN for records held within the IMPACT business areas allows for the all the information known on a person across the different business areas to be linked. Although this may not be possible in every force at present, the initiation of this referencing will allow for information to be managed more effectively both at force and national level.

PNC is a source which can help confirm a person's identity. Checks should be made on the PNC to establish whether a person is already known to the Police Service. PNC name checks alone should not be the only method of verification and cannot be relied on solely for correct identification. Biometric data, such as fingerprints, DNA or recorded marks and scars, should be used to confirm a person's identity where possible. If a PNC record can be accurately linked to a person record, then a cross-reference should be made on the person record to the PNC ID.

The delivery of the IMPACT Police National Database (PND) will provide a capability to search people records nationally. For further information on the IMPACT programme, see **http://www.npiaextranet.pnn.police.uk/microsite/impact/index.html**

4.6 Responsibilities

4.6.1 Managers

- Ensure data quality is treated as a priority;
- Ensure there is the ability to link and cross-reference information across the different business areas;
- Ensure that staff responsible for recording police information are trained in accordance with the National Training and Delivery Strategy.

4.6.2 Supervisors

- Perform a regular dip sample of records to ensure that they comply with data quality and recording principles;
- Ensure staff are recording information in the appropriate format;
- Provide feedback to staff on record creation.

4.6.3 Users

All staff are responsible for recording information for a policing purpose. Staff should:

- Record information in the appropriate format;
- Record information in compliance with the recording and data quality principles;
- Make all necessary efforts to ensure person records are unique.

Checklist 1

Recording Police Information

- Ensure information is recorded for a policing purpose;
- Ensure information is recorded in the appropriate format for the business area in which it is held;
- Ensure information is recorded according to the data quality principles – accurate, adequate, relevant and timely;
- Ensure checks are made to avoid creating duplicate records;
- Ensure links are made to existing records;
- Ensure correct GPMS marking.

5

Evaluation and Actioning of Police Information

This section describes the process for evaluating and actioning police information.

Key principles of this section are:

- **Information will be evaluated and risk assessed for its accuracy, value and sensitivity;**
- **Evaluation allows for action to be determined and priorities to be identified;**
- **Evaluation allows for the identification of links with other police information recorded elsewhere.**
- **Evaluation enables the quality assurance of police information;**
- **Information recorded through the 5x5x5 process will undergo evaluation by the relevant intelligence unit;**
- **Evaluation should be proportionate to the nature of the information.**

Contents

5.1 Why Evaluate Police Information?

Police information will undergo a form of evaluation appropriate to the policing purpose for which the information was collected and recorded. All police information is evaluated to determine its provenance, accuracy, continuing relevance to a policing purpose and what action, if any, should be taken. Provenance is the ability to determine the reliability and credibility of the source, and the value of the content of the information.

The evaluation process determines the type of action that should be taken on the information. Action may include an immediate response, further development of the information, whether to share the information with others or deciding not to do anything with the information at that time, subject to review.

Evaluation involves searching and making connections with other records. This may require staff to search the different business areas.

Evaluation should be proportionate to the nature of the information. For example, an incident record will be evaluated quickly to determine the urgency of response required. A crime in action would normally require a faster response than an abandoned vehicle report. A series of reports relating to similar events or situations might, however, require a more in-depth analysis to see if they represent a pattern. For example, a series of reports of fires being started at particular locations might warrant details being entered onto an Information/Intelligence Report.

5.2 Principles of Evaluating Police Information

When evaluating any police information, the following principles apply regardless of the business area where the information is held:

- The provenance, accuracy and reliability of the information should be established;
- Provenance will include assessment of the reliability of the source, risk to the source and subject, risk to the storage and use of the information;
- A risk assessment will apply where appropriate;
- A decision will be made whether to sanitise the police information where the source or content is sensitive;
- Identify links between different records;
- Information will be assessed for its intelligence value;
- A priority assessment can be applied.

5.3 How Police Information Is Evaluated

Police information is evaluated in accordance with the format in which it was recorded and the business area where it is held. Alongside the general principles in **5.2 Principles of Evaluating Police Information,** specific evaluation criteria apply to the following business areas.

5.3.1 Crime Recording

Most forces will have a central crime reporting capability and local crime management units. Local force policies will determine the processes by which reports of crime are assessed and evaluated. It is also important to ensure that there are processes to ascertain the accuracy of the report, and that records of these processes are maintained.

All forces are required to comply with the NCRS as outlined in **4.4.1 Crime Recording.** Crime reports are a key business management information source. Crime records and their standards are primarily concerned with investigating and recording crime rather than evaluating the information contained in them. It is essential that all crime records are created in compliance with the NCRS and are available to aid further development and become a source of information.

By evaluating crime reports, information can be identified which may have an intelligence value. Crime reports have personal details of victims and witnesses and, if known, offenders. Details of crime location, offending methods (MO) and times of offences are also recorded. This evaluation may occur automatically but, in other circumstances, the information may need to be recorded onto a 5x5x5 for input into the intelligence business area.

5.3.2 Domestic Abuse

Domestic abuse records (like crime reports) contain details of victims, witnesses and suspects/offenders. Due to the sensitivity and high-risk nature of the information, it is particularly important that records are properly evaluated to ensure appropriate responses. Key risk factors may include:

- History of previous incidents;
- Potential risk to children;
- Dynamic factors, for example, dispute over custody of children.

For further information see ***ACPO (2008) Guidance on Investigating Domestic Abuse.***

5.3.3 Child Abuse Investigation

Records of child abuse investigations are particularly sensitive because of the age of the victim and the seriousness of the offending. The vulnerability of a child as a potential witness may also mean that it may be considered not to be in their best interests to proceed to prosecution. In all cases the information must be linked to the suspect to identify patterns of repeat offending. Evaluation should ensure that details of suspected or known offenders are captured along with details of their MO. For example, abuse of trust or any evidence of grooming.

For further information see ***ACPO (2009) Guidance on Investigating Child Abuse and Safeguarding Children,*** **Second Edition.**

5.3.4 Public Protection

Public protection information is sensitive and high risk and, therefore, requires rigorous evaluation and risk assessment. Linking information about public protection to the intelligence system will achieve this. In most forces public protection records are already recorded using the 5x5x5 reporting system. Where this is not yet the case, there should be a marker on the intelligence system to indicate the existence of a public protection record.

All information relating to threats to public safety should be recorded on a 5x5x5 because of the risk to the source and the public.

See **4.4.4 Public Protection** for the definition of public protection, as it relates to this guidance.

5.3.5 Missing Persons

Records created in this business area generally focus on the details and circumstances of the missing person. It is particularly important, therefore, that the subsequent evaluation process identifies and records any relevant links to any other business areas.

For further guidance see ***ACPO (2010) Guidance on the Management Recording and Investigation of Missing Persons,*** **Second Edition.**

5.3.6 Case and Custody

The details of people in police custody are an important source of information that may have an intelligence value. It is essential that the personal details of all detainees are verified to ensure the accuracy of the person record. Any details held on the custody record, for example, visitor details, contact telephone numbers or unique characteristics of the detainee should also be considered in relation to its possible intelligence value. This evaluation may occur automatically but, in other circumstances, the information may need to be recorded onto a 5x5x5 for input into the intelligence business area.

5.3.7 Incident Records

An incident report is usually the first record relating to a particular crime or incident. Once the report is recorded, it should be considered and evaluated for its intelligence value. Forces should comply with the NSIR when recording incidents.

Calls from the public for assistance or reports of incidents are initially managed through force or BCU command and control systems. Such reports are evaluated for their accuracy before being assessed for the level of policing response necessary. Incident reports are also managed through a priority assessment process, identifying the urgency of the response required. For further information on the standards which apply, see **http://www.homeoffice.gov.uk/rds/countrules.html**

Many forces have adopted an immediate incident research capability or bureau (IRB). The IRB is responsible for conducting immediate research on the details of incident reports relating to high-risk issues, by examining all other business area records relevant to the report. The IRB ensures that all officers attending incidents are informed of any risks they are likely to face on attending the location or dealing with the subject of the report.

5.3.8 Firearms Licensing

Information contained in the NFLMS will be subject to the principles of evaluation in **5.2 Principles of Evaluating Police Information.** The information held within this business area may link to records held in other business areas and could provide potential intelligence, for example, the reasons for a firearms licence revocation.

5.3.9 Intelligence

The 5x5x5 is part of the evaluation process and is central to managing the risk attached to that record. The 5x5x5 establishes the provenance of the information and the reliability of the source which, in turn, influences how the information should be handled and disseminated. This process is fundamental to:

- Evaluating individual intelligence records;
- Action management;
- The ultimate integrity of the intelligence business area as the key location for information about known or suspected criminals.

The evaluation role is usually performed by the intelligence unit. It is good practice for the process of recording and evaluating intelligence records to be undertaken in two stages: where one person is responsible for recording the information on a 5x5x5, and the other is responsible for the quality assurance and evaluation role.

The evaluation of intelligence records against information held in other business areas provides further quality assurance for action management. This evaluation process is integral to NIM; see ***ACPO (2005) Guidance on the National Intelligence Model.***

For further information on the 5x5x5 evaluation process, see **Appendix 2.**

5.4 Action Management

The evaluation of information enables priorities to be identified and the appropriate action to be taken. An action management process is the means of identifying whether an immediate response is needed, for example, a threat to life or significant risk to the public.

Actioning any police information results in one of the following responses:

- Initiating a response – this could include an immediate operational response to the information, a decision to share the record with other partners, or a referral to the tasking and co-ordination group. If the information is likely to lead to an investigation, the principles of all investigations are outlined in ***ACPO (2005) Practice Advice on Core Investigative Doctrine.***

- Generating further research and development – this could include the development of intelligence products.

- Making a decision not to do anything; but to review the information at a future date.
- Deciding to take no action.

The process of decision making is set out in NIM. This describes the development of intelligence products, the tasking and co-ordination process, and the allocation of resources.

For further guidance on the decision-making process, see ***ACPO (2005) Guidance on the National Intelligence Model.***

5.5 Responsibilities

5.5.1 Managers

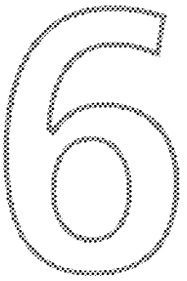
- Ensure that the intelligence business area is robust, reliable and relevant;
- Follow the principles of NIM;
- Ensure that the staff responsible for evaluating police information are trained in accordance with the National Training and Delivery Strategy.

5.5.2 Supervisors

- Oversee the quality assurance process for accuracy, adequacy, relevancy and timeliness;
- Perform a regular dip sample of records created in their business area to ensure the 5x5x5 is being used where necessary;
- Ensure the proper completion of the 5x5x5 in line with this guidance.

5.5.3 Users

- Quality assure the recording of the 5x5x5 and ensure the linking of information where relevant;
- Identify opportunities for analysis of series or linked events;
- Apply provenance to the information recorded;
- Apply relevant priority assessment if appropriate;
- Disseminate information where appropriate.



Information Sharing

This section provides guidance on the information sharing process and emphasises the importance of sharing police information with others.

Key principles of this section are that:

- **Policing requires information to be shared within the Police Service, with partner agencies and the public.**
- **Police forces should actively seek to share non-personal information. Personal information should also be shared but is subject to certain safeguards which all police staff should be aware of.**
- **Establishing a policing purpose and a legal gateway is the basis for sharing police information.**
- **Information sharing agreements between the police and partner agencies should be used to ensure consistent and proportionate sharing.**

Contents

Contents

6.1 Why There Is a Need To Share Police Information

Information sharing refers to the processing of information, either on a one-off or an ongoing basis between partners for the purpose of achieving a common aim.

Effective policing relies on the Police Service to communicate and share information with a wide range of partners. Information sharing:

- Can help to deliver improved public services;
- Leads to an increased openness among partners, which, in turn, builds confidence and trust in the Police Service;
- Is a two-way process that enables links to be made between people, objects, locations and events that would not be possible otherwise;
- Increases expertise, professionalism and an understanding of the process of sharing information;
- Enables partners to make informed decisions about how best to protect the public.

While there are clear advantages in sharing information with others, information can only be shared where it is lawful to do so. Information should not be shared purely as a matter of routine. Each case should be viewed individually with informed decisions made about whether to share or not.

Nothing in this section conflicts with any existing arrangements to protect sensitive information.

This guidance does not cover disclosure of material in connection with criminal proceedings as defined under the Criminal Procedure and Investigations Act 1996.

6.2 Information Sharing Landscape

There are three main scenarios where police information can be shared:

- Required by or under statute (statutory obligation);
- Permitted by or under statute (statutory power);
- Using common law.

Further detail on these categories can be found in **6.3 Statutory Obligation** to **6.5 Common Law.**

6.3 Statutory Obligation

The term statutory disclosure applies where there is a specific legal obligation to disclose police information to another party.

Examples of statutory disclosures include court orders, the Notifiable Occupations Scheme and disclosures to the Child Support Agency and the Criminal Records Bureau (CRB).

Where there is a frequent and continuing need for the Police Service to disclose information then forces, with their partners, should develop a memorandum of understanding (MoU), an information sharing agreement (ISA) or a service level agreement (SLA). These should clearly set out the statutory obligations of the organisations involved, together with the procedures to ensure effective, timely and consistent disclosure.

There are a number of national MoUs that have been developed by ACPO, on behalf of the Police Service, with government organisations. Where these exist, they should be used and forces need not develop their own.

Key schemes where the Police Service is obliged to disclose information include the following.

6.3.1 Disclosure under Part V of the Police Act 1997

The Police Act 1997 creates a statutory scheme for the disclosure of criminal records and police information on potential employees to prospective employers. The CRB is responsible for the scheme and for ensuring that employers have sufficient information to make a judgement on the suitability of a potential employee to work with children or vulnerable adults.

The CRB and ACPO have a Disclosure Quality Assurance Framework (QAF) to help to ensure consistency between forces on the disclosure of information by the police to the CRB. It does this by:

- Documenting which police business areas are to be searched and under what circumstances;
- Standardising the criteria used to decide if information in a police business area is potentially relevant;
- Standardising the criteria used to decide if disclosure is appropriate;
- Ensuring the rationale for decision making is recorded.

For further information on the CRB disclosure scheme, see the CRB website at **http://www.crb.gov.uk/**

6.3.2 Notifiable Occupations Scheme

Information relating to this scheme can be found in **6.5.2 Notifiable Occupations Scheme.**

6.3.3 Independent Safeguarding Authority Schemes To Protect Children and Vulnerable Adults

The Independent Safegaurding Authority (ISA) was created in 2009 and has four statutory duties. These are to:

- Maintain a list of individuals barred from engaging in regulated activity with children;
- Maintain a list of individuals barred from engaging in regulated activity with vulnerable adults;
- Make well-informed and considered decisions about whether an individual should be included in one or both barred lists; and
- Reach decisions as to whether to remove an individual from a barred list.

The ISA replaces PoVA, PoCA and List 99 with two lists:

- The ISA Children's barred list;
- The ISA Vulnerable Adults barred list.

For further information about the ISA see
http://www.isa-gov.org.uk

6.3.4 Disclosures Under the Freedom of Information Act 2000

Section 1 of the Freedom of Information Act 2000 (FOIA) provides individuals with a statutory right to access information held by public authorities (including police forces). Members of the public have a right to be told whether or not the police force holds the information sought and, if so, to have the information communicated to them.

There are exemptions to FOIA disclosures; more information about this can be found in ***ACPO (2008) Freedom of Information Manual of Guidance*, Version 5.** This manual also describes the standards which all forces are expected to adopt to ensure a consistent approach across the Police Service to manage the right of access to information provided by the FOIA.

6.3.5 Disclosures Under the Data Protection Act 1998

Sections 7 to 9A of the Data Protection Act 1998 (DPA) provide individuals with a statutory right of access, commonly known as Subject Access, to their personal data held by forces. The most important element of this right is the entitlement to be provided with a copy of their personal data within a forty day statutory time limit.

This is subject to certain exemptions, further information can be found in ***ACPO (2009) Manual of Guidance on Data Protection,*** which also identifies the other disclosures provided by the DPA and describes the standards which all forces are expected to adopt to ensure a consistent approach across the Police Service.

6.4 Statutory Power

The term statutory power applies where there is a specific legal power, but not an obligation, to share police information with another party.

The Police Service shares a common purpose for managing information. This means that forces can share information with one another without the use of information sharing agreements, memorandums of understanding or service level agreements.

When sharing information within the Police Service, it is important that there is an audit trail of the identity of the person requesting the information and of the information that is being shared.

Some systems such as the PNC, ViSOR and the NFLMS facilitate information sharing at a national level. The PND will add to these capabilities.

There is a clear legal distinction between making police information available within the Police Service and making it available to other parties. For the purposes of this guidance, the Police Service includes those forces defined in section 1 of the Police Act 1996, the Serious Organised Crime Agency (SOCA), and other forces not covered by section 1 with whom separate arrangements exist.

The Police Service also shares and receives information with people outside the police. This subsection focuses on information sharing with partner agencies, which fall into two broad categories: those that have a statutory purpose to share or receive information and those that do not.

6.4.1 Other Types of Sharing Where a Statutory Power Exists

Before sharing information outside the Police Service, it should first be determined whether a statutory purpose exists for that information sharing. Where the police are requested to share information with a partner that will be used, for example, to protect a child, the agency receiving that information must identify a legal power that allows them to lawfully request and process it.

Using the example given, section 47 of the Children Act 1989 allows for social services to request information from other agencies as part of an ongoing child protection inquiry. Similarly, section 115 of the Crime and Disorder Act 1998 gives the power to share information within Crime and Disorder Reduction Partnerships and Youth Offending Teams for crime prevention purposes and other purposes specified by that Act.

For further information see **http://www.crimereduction.gov.uk**

6.5 Common Law

Where the police are requested to share information with a partner and a statutory obligation or power does not exist, a policing purpose should be established as the decision to share is risk based, and should take into account the source of the information and any restrictions on its onward dissemination. This should be balanced against the requirements of the common law duty of confidence, the Human Rights Act 1998 and the Data Protection Act 1998. For example, a police force which plans to share information on known hooligans with a football club so that the club can ban them from attending football matches, should first establish a policing purpose for doing so.

In cases where the police wish to share information about sexual offences with schools or other educational establishments, an officer of ACPO rank should make the decision to share, balanced with the requirements of the HRA and the DPA.

6.5.1 Dissemination

The term dissemination in this context is usually applied to the passing of intelligence records from one agency to another, or from one department to another. It occurs when the holder of the material recognises its potential significance to another party. Dissemination may involve sanitisation of the original information and/or the imposition of certain conditions restricting its further dissemination or use without reference to the originator.

The process for dissemination of intelligence records is described in detail in **Appendix 2.**

6.5.2 Notifiable Occupations Scheme

The Notifiable Occupations Scheme relates to professions or occupations that carry special trust or responsibility. Here the public interest in the disclosure of convictions and other information by the police generally outweighs the normal duty of confidentiality owed to the individual.

Checklist 2

Sharing Police Information

- Where a statutory provision exists, this provides a specific purpose for sharing police information with an outside agency.
- Where a statutory provision does not exist, the decision to share is based on establishing a policing purpose and undertaking a risk assessment.

6.6 How the Police Share Information

The decision to share information requires careful judgement in which data protection and human rights considerations are balanced with policing purposes. Any information that the police are considering sharing with a partner agency should, therefore, be necessary for the purpose for which it is being shared.

The following principles in this subsection help to determine whether the information the police are considering sharing is necessary, and are specific to personal data only.

Non-personal data is not subject to the same tests or considerations. Sharing of non-personal data is widespread, for example, making available details of burglaries in a specific area to a Neighbourhood Watch group. In considering requests for police information, thought should be given as to whether it is lawful and necessary to disclose any personal information.

6.6.1 Police Information Must Be Accurate

Police information must be accurate and care should be taken to ensure that it remains relevant for the purpose for which it is being shared. The police may also share information that has been recorded by another agency. Where this occurs, special care should be applied to its validity to ensure that it is both relevant and complies with the principles contained in the DPA. Any conditions imposed by the originating agency should be observed before sharing takes place.

6.6.2 Police Information Must Be Judged on its own Merits

The relevance of a specific record should be decided on a case-by-case basis. For example, it may not be necessary to share details of all information held about a particular individual, including details of acquittals or convictions not recorded on the PNC or elsewhere.

There may be instances in which other information comes to light that makes an earlier record more relevant. For example, the age of the victim of a sexual assault may not be apparent from the record of conviction on PNC, but may be relevant to the request for information, particularly if there is a large age gap between the offender and victim.

The police may also consider it relevant, in certain circumstances, to provide a partner agency with information that falls outside the request. For example, information might be shared about a person who resides or associates with an individual, as this may help to build a more complete picture for the partner agencies such as whether a child is living at the same address as a convicted sex offender.

6.6.3 Relevance Should Be Clearly Explained

When sharing information, the relevance of the information to the request should be clearly explained. Sufficient information should be provided to the partner agency to ensure that it is meaningful without making it difficult to read or understand.

Having made a decision on whether the information is relevant for the purpose for which it is being shared, the decision should be recorded against the record so that it can be audited at a later date.

6.7 Considerations When Sharing Personal Information

Information sharing must be carried out within the existing legal framework. Where there is an absence of a specific duty to share, a power or policing purpose will usually need to be identified. This means that the legal obligations for processing information under common law, the DPA and the HRA should be considered before sharing can take place.

6.7.1 Proportionality

In considering whether to share personal information, forces should ensure that a fair balance is achieved between the protection of an individual's rights and the general interests of society. Sharing personal information may be proportionate if:

- The individual concerned consents to the information being shared; or
- The purpose justifies infringing the right to privacy; and
- The measures taken to meet the purpose are rational and fair;
- The means used to share are no more than is necessary to accomplish the purpose.

There is a lower threshold to meet the test of proportionality when sharing factual information. There is a higher threshold to share personal information about less serious crimes as there is a lower public interest in this information being exchanged.

This means that police officers will need to ensure, on a case-by-case basis, that the information they are considering sharing is in the public interest and is proportionate, necessary and meets a legitimate aim under Article 8 of the European Convention on Human Rights (ECHR). It is significant that any public authority (for example, a local authority) will be bound by the same obligations under the HRA as the Police Service.

6.7.2 Data Protection Act 1998

The DPA provides a framework for decision-making in relation to personal or sensitive personal information. The DPA places a requirement on chief officers to process information in compliance with the eight principles set out in **1.4 Legal Basis for Managing Police Information.**

Further information on the DPA can be found in ***ACPO (2009) Manual of Guidance on Data Protection.***

6.7.3 Common Law Duty of Confidence

The common law duty of confidence applies where information of a personal or sensitive nature is collected and recorded. A breach of confidence will apply when the information collected and recorded is used in an unlawful manner. There are, however, a number of exceptions to the duty, specifically:

- Where there is a legal requirement (either under statute or a court order) to disclose the information;
- Where there is an overriding duty to the public (for example, where the information concerns the commission of a criminal offence or relates to life-threatening circumstances);
- Where the individual to whom the information relates has consented to the sharing.

The police also owe a duty of confidentiality to victims and witnesses of crime, who may expect a greater level of privacy than offenders. A balance, therefore, needs to be struck between sharing such information and the rights of victims and witnesses to privacy.

In certain circumstances consent does not need to be sought. For example, where the request to share meets a policing purpose and does not compromise operational procedures or an individual's safety. An assessment of the vulnerability of those at risk and the impact of the disclosure on the individual will need to be made before making a decision whether to seek consent.

6.8 Sharing Through an Information Sharing Agreement

Information Sharing Agreements (ISAs) – also known as Information Sharing Agreements or Protocols – should be used when the police request or are requested to share information with others. **(Information Sharing Agreements should not be confused with the Independent Safeguarding Authority which shares the acronym ISA.)**

> **Note:** Some forces use the terms Memorandum of Understanding (MoU), Information Exchange Agreement (IEA) or Information Exchange Protocol (IEP). In the context of MoPI these terms are interchangeable with ISA.

An ISA is a formal arrangement between organisations who wish to share personal information held and managed centrally within force. The IMS should clearly state where ISAs are stored and who is responsible for their maintenance.

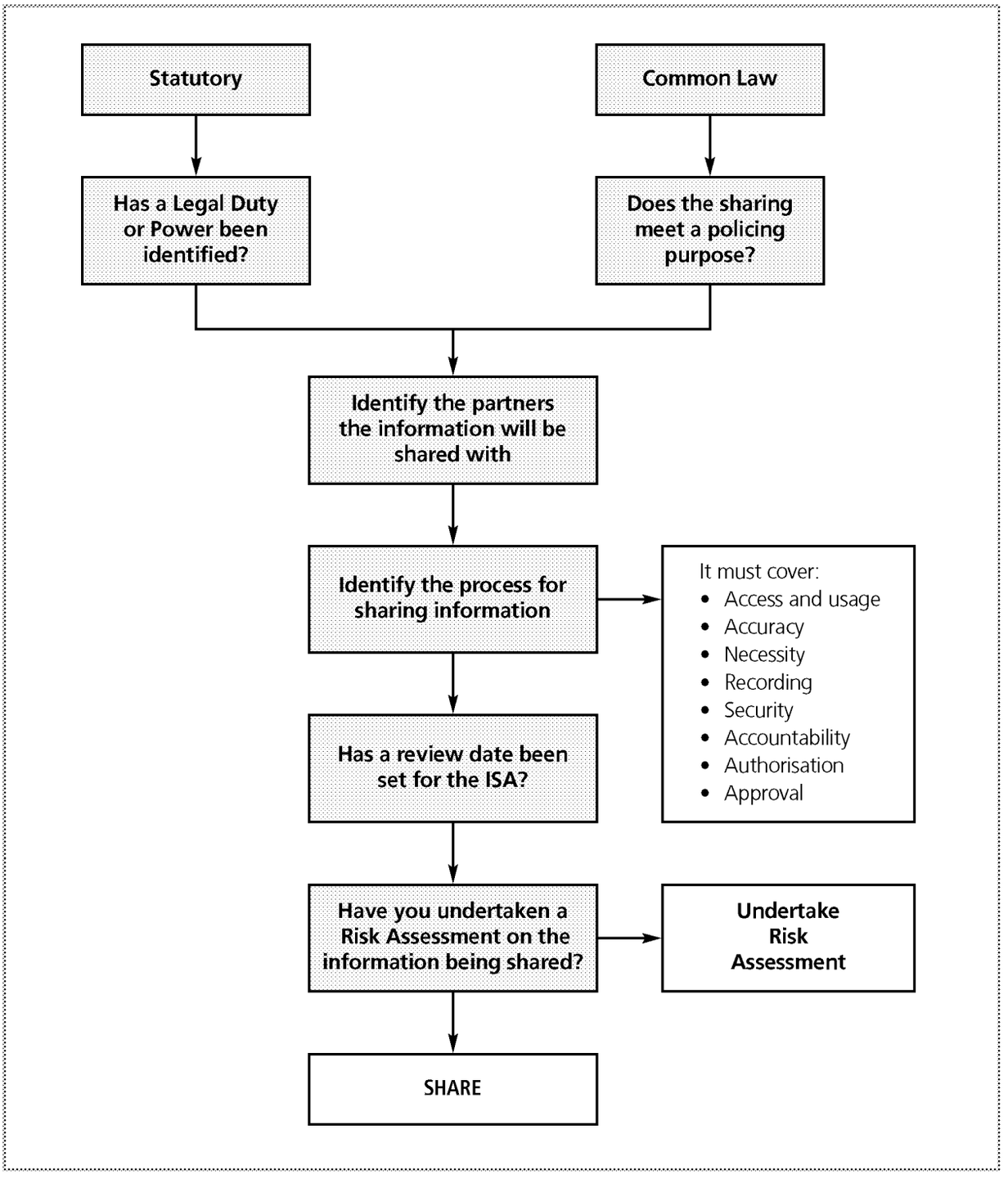
Establishing ISAs with partners has a number of advantages. In particular, they:

- Ensure consistency in the way information is shared;
- Allow the police to place conditions on the way information will be handled by the partner agency and vice versa;
- Ensure that information can be shared lawfully;
- Help build confidence in the role that the police play in protecting the public.

An ISA does not stop the ability to place conditions on the sharing of sensitive information between the police and other partners where appropriate.

The flow chart on the following page sets out the process of developing an ISA. Where ISAs already exist, the flow chart can be used to check that the existing arrangements enable consistent and lawful information sharing.

Figure 1 – Information Sharing Agreement (ISA) Process Chart



6.8.1 Establishing a Policing Purpose or other Legal Power

Once a need or request for sharing information has been identified, it will be necessary to ensure that the sharing is in accordance with a legal power (such as section 115 of the Crime and Disorder Act 1998), or that it meets one of the policing purposes set out in the ***MoPI Code of Practice.*** This is the most important step in the process as, without it, it will not be possible to share information lawfully.

6.8.2 Identifying the Partner to the Agreement

Details of the partner agencies, and names, addresses and contact details should be recorded in the agreement. Identifying partners in the agreement also helps to confirm whether the partner can rely on a statutory purpose to request information or whether the decision to share is based on risk and, therefore, requires a policing purpose to be established.

6.8.3 Setting Out the Process for Sharing Information

Setting out in the agreement the process for sharing is particularly important. It provides those involved in the process with a clear understanding of how the information will be shared, with whom and when. It also represents an opportunity for forces to place conditions on how the partners may use the information and should form part of the agreement itself. The following questions should be asked when developing an ISA.

What information is being shared?

The ISA will need to set out the type of information being shared. This could include details of individuals, convictions, cautions or other information. It may also be necessary to identify where the information is kept. (Any information being shared should, however, be proportionate and necessary for the purpose for which it is being shared.)

Who will have access to the information and what may they use it for?

The police may wish to identify individuals or business areas within partner agencies that will have access to the shared information, particularly if it is sensitive information that may compromise an operation or place an individual at risk. The police may wish to look at any vetting or confidentiality agreements the partner agency may have in place to counter this. Furthermore, the police may also want to ensure that the partner has a policy for the storage of information. Where the police share information with others who do not recognise the GPMS, the decision as to who has access and what they may use it for, is a risk-based decision.

How will the information being shared be kept accurate and up to date?

Police forces are responsible for ensuring that any information they share is accurate and current, in line with existing national or local standards set out in the IMS.

For how long a period will the information be retained?

The ISA can be used to specify when the information the partner received should be reviewed and subsequently retained or disposed of. This should be undertaken in line with force review, retention and disposal policy contained in the IMS.

How will the information being shared be recorded?

Procedures should be in place to ensure that any information sharing is recorded and documented in a registered file. A file needs to be kept to ensure that the process can be audited at a later date, and to aid the review part of the process.

How is the security of the information being shared ensured?

The agreement can be used to apply a protective marking to the information being shared in line with the GPMS, where applicable. There may also be a need to apply other safeguards to the processing of information that may affect its transit or storage at a partner's site.

Who is accountable for the ISA?

Every individual involved in the drafting of an ISA has a responsibility to ensure that the information being shared is processed in compliance with the law and with national standards. Where possible, the names of the individuals responsible for the development of the ISA within forces and partner agencies should be clearly stated on the registered file.

Who will approve and authorise the ISA?

Once the ISA has been finalised, the Police Service and partner agencies should ensure that they fully understand and agree with the purpose, process and conditions of the agreement. Approval within the Police Service will normally come from a business area owner. Signature to the agreement should come from a senior member of staff, typically an ACPO rank officer or a person delegated by them. In partner agencies, the signatory should also be a senior member of staff who can be held accountable for the processing of information.

How will forces ensure compliance with the Data Protection Act 1998 if the information being shared is personal or sensitive personal information?

Whenever personal information is held by an organisation, it must be processed in accordance with the eight principles of the Data Protection Act 1998.

Where will the ISA be held?

All ISAs should be held centrally and made available to staff on the force intranet. A high-level summary of the agreement can be added that provides a brief description of the purpose, partners and process together with the name of the individual who is tasked with maintaining the agreement.

ISAs should also be made publicly available, where possible. The process for sharing information should be kept as transparent as possible as this will encourage partner agencies to seek further opportunities to share information.

Providing these questions have been answered, are clearly explained in the document and recorded, then information sharing can take place.

6.8.4 Sharing within an ISA

An ISA provides a framework to facilitate confidence in information sharing. It should not be viewed as a bureaucratic obstacle to be overcome before any information sharing can take place. For example, where the police are involved in a partnership arrangement with another agency, it would normally be appropriate for an ISA to be in place, but individuals working within the partnership (such as a police officer within a local authority) should not feel constrained to fill in a form every time they speak to a colleague.

6.9 Review

Review is an essential part of any ISA. The aim of a review is to ensure that the agreement is achieving its purpose and the actual process of sharing is operating smoothly. It should be carried out by the force data protection officer in conjunction with partner agencies and be performed on an annual basis, except where the agreement is in its first year when it should be reviewed after the first six months.

The following stages set out the process of review.

6.9.1 Does the Agreement Have the Right Contact List?

Each signatory organisation has a responsibility to maintain up-to-date contact details of the key individuals operating or managing the sharing activity. When a change in personnel occurs, the partner in question should ensure that the other partners are made aware of the change and adjust the agreement accordingly.

6.9.2 Is the Agreement Still Useful and Fit for Purpose?

A review represents an opportunity to test whether the agreement is still useful and whether the purposes for which it was established are relevant. Some agreements may have been created for a specific purpose that no longer exists. Others may be a long-term commitment to share. If partners decide that the agreement is no longer useful, it should be terminated.

Consideration should also be given to whether the correct information is being shared at the right time as specified in the agreement. A review may identify a need for adjustment to reflect the changing needs of the Police Service or a partner agency. Any changes, however, will need to be approved by each partner agency and recorded accordingly. Where this occurs, an addendum with agreed modifications should be added to the ISA. Alternatively, if there are substantial amendments to the original ISA, a new ISA may be necessary.

6.9.3 Has the Review Identified any Emerging Issues?

Reviewing the agreement provides an opportunity to discuss any problems that may have arisen during the period of review. There may be concerns about the way in which the information has been shared or that the information has been used in a different way than was intended.

Another significant issue relates to legislative changes. Reviewers will need to be aware of any amendments to existing legislation or any new legislation enacted that may have an impact on the agreement. Again, any changes will need to be recorded, approved and added in an addendum.

Finally, a review may also identify gaps where an opportunity to share information would help to achieve one or more of the policing purposes.

6.9.4 Extending/Terminating the Agreement

At the end of the review, a decision should be made on whether to extend the agreement for a further period (typically one year) or whether to terminate it. Any decision should be recorded, clearly stating the reasons for choosing a particular course of action.

6.10 The Process of Sharing Police Information Outside an ISA

Where an ISA does not exist, or the decision to share is a one-off, the following checklist provides a reminder of the key questions that will help to ensure any information sharing is lawful.

Checklist 3

Sharing Information outside an ISA

- Who is asking for the information?
- Have the name, position, organisation and contact details of the person asking for the information been recorded?
- Has the identity of the person requesting the information been verified?
- What information is being asked for? What purpose will it be used for?
- Is the information being requested personal information?
- Does a statutory or common law provision exist, and has a policing purpose to share information been established?
- If yes, how do they want the information?
- When do they want the information?
- Once information has been shared; record the decision, why it was made, and what information was shared.

6.11 Responsibilities

6.11.1 Managers

- Supporting staff to share information appropriately;
- Providing a system for recording decisions on whether or not to share information;
- Ensuring that all ISAs are held and managed centrally within force;
- Ensuring that the process of sharing information is adhered to by those in a supervisory and user capacity;
- Authorising ISAs;
- Ensuring that staff who have a responsibility for sharing information are trained in accordance with the National Training and Delivery Strategy.

6.11.2 Supervisors

- Supporting staff to share information appropriately;
- Auditing, on an ad hoc basis, the decision to share made by users, including the necessity, accuracy and adequacy of information shared;
- Checking whether the decision to share meets a policing purpose or other legal duty or power;
- Ensuring that information being shared does not compromise any police operation or the safety of others;

- Ensuring that a risk assessment process is adhered to by the user when making a decision to share information;
- Ensuring that ISAs are reviewed in accordance with force policy;
- Providing feedback to staff on their performance.

6.11.3 Users

- Ensuring that information is relevant, accurate and adequate for the purpose for which it is being shared;
- Ensuring that when personal information is shared, the requirements of the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidence have been fulfilled;
- Applying a protective marking to the information being shared under the GPMS where applicable, or carrying out a risk assessment where the sharing is with the partners in the voluntary or private sectors who do not have a statutory purpose to share information;
- Recording decisions to share or not to share information in accordance with the IMS;
- Ensuring that the information being shared is lawfully disclosable for a statutory purpose and is proportionate and necessary to achieve a policing purpose;
- Following existing force policies set out in the IMS that comply with this guidance.

7

Review, Retention and Disposal

This section explains what is meant by the terms review, retention and disposal. It provides guidance on the timeframes for reviewing information and the criteria used for deciding whether to retain the information or dispose of it.

Chief officers are required to balance resources against local policing needs. In this context, chief officers should develop risk-based review, retention and disposal policies and procedures which have regard to this guidance document and the *MoPI Code of Practice,* while also taking into account the resources available to the force and other policing demands.

Key principles of this section are:

- **The review of police information is central to risk-based decision making and public protection;**
- **Records must be regularly reviewed in order to ensure that they remain necessary for a policing purpose, and are adequate and up to date;**

- **Forces are responsible for reviewing their own records;**
- **The type and amount of information held on an individual must not be excessive and must be proportionate to the risk they pose to the community;**
- **The review process should be documented for audit purposes;**
- **Records should be disposed of when there is no longer a policing purpose for retaining them.**

Contents

7.1 Why Review Police Information?

The primary purpose of review, retention and disposal procedures is to protect the public and help manage the risks posed by known offenders and other potentially dangerous people.

Reviewing information held by forces to determine its adequacy and continuing necessity for a policing purpose is a reliable means of meeting the requirements of the Data Protection Act. Review procedures should be practical, risk focused and able to identify information which is valuable to the policing purpose and needs to be retained. Review procedures should not be overly complex but should be as straightforward as is operationally possible.

This guidance is principally concerned with the process for reviewing personal information covered by the Data Protection Act. Review of non-personal information is not explicitly covered although it is good practice to apply the principles of this guidance.

To manage risk effectively the Police Service should have standard procedures in place for reviewing records and making informed, accountable decisions on the retention or disposal of information. Review procedures ensure that information retained by the Police Service is held lawfully, and may help to prevent forces being overloaded by the volume of information captured and recorded.

Other key drivers are within common and statute law, particularly the eight principles of the Data Protection Act. A failure to review and retain information appropriately may be unlawful and undermine public confidence in the Police Service.

The guidance provided in this section relates to information held on all police systems other than the PNC. The review, retention and disposal of information on the PNC should be conducted in accordance with the PNC Retention Guidelines. It should be noted that the step-model, which forms the basis of the PNC Retention Guidelines is, by nature, a review process. There is no additional requirement to further review records held on the PNC unless an exceptional case requires this to be undertaken.

7.2 Legal Issues

There are a number of specific legal provisions that are relevant to the review, retention and disposal of police information. These are summarised in **7.2.1. Human Rights Act 1998** to **7.2.4. Freedom of Information Act 2000.**

7.2.1 Human Rights Act 1998

Public authorities, including police forces, must act in a way that complies with the European Convention on Human Rights (ECHR) and the Human Rights Act 1998. In relation to record retention this requires a proportionate approach to the personal information held about individuals. The decision to retain personal records should be proportionate to the person's risk of offending, and the risk of harm they pose to others and the community. A higher proportionality test should be met in order to retain records about relatively minor offending.

Case law places a heavy responsibility on the Police Service to ensure that certain categories of police information are not routinely shared outside the Police Service 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 the Police Service.

7.2.2 Data Protection Act 1998

Records of personal information that comply with the Data Protection Act 1998 (DPA) principles can be held lawfully by the Police Service. All other legal requirements governing the handling of personal records should be considered secondary to the DPA. This is because any record containing personal information that does not comply with the DPA must be either amended or disposed of.

Compliance with the DPA principles will assist forces in their compliance with other relevant legislative requirements. For further information see **1 The Purpose of Managing Police Information.**

7.2.3 Criminal Procedure and Investigations Act 1996

The Criminal Procedure and Investigations Act 1996 (CPIA) has established requirements for retaining information relevant to investigations for set periods of times. It states that relevant information must be retained at least until:

- A decision is taken whether to institute proceedings against a person for an offence;
- The accused is convicted, acquitted or the prosecutor decides not to proceed with the case;

- The convicted person is released from custody or hospital, in those cases where a custodial sentence or hospital order is imposed;
- Six months from the date of conviction in all other cases.

Note: The retention periods set down by the CPIA are a minimum requirement and, in most cases, the retention requirements outlined in this guidance will far exceed those imposed by the CPIA. Information should still be retained for as long as it is necessary and proportionate to do so, irrespective of the CPIA requirements for it. For example, the PNC will hold all conviction data until the record subject is deemed to have reached 100 years of age, regardless of how long this information is required for CPIA purposes.

7.2.4 Freedom of Information Act 2000

The FOIA encourages accurate record keeping. A request under the FOIA does not mean that records cannot be updated once the information has been disclosed.

Section 77 of the FOIA makes it an offence to deliberately alter or erase records once an application for access to them has been made in an effort to avoid having to disclose them. This means that forces may have to disclose any records that they hold, even if these records are inaccurate, excessive or otherwise contravene the Data Protection Act 1998. It is, therefore, imperative that all records are reviewed for necessity and adequacy so that they can be confidently disclosed if required.

7.3 Definitions

There are three key terms essential to the review process: Review, Retention and Disposal. They are defined below.

7.3.1 Review

To examine a person record and all associated records, to ensure:

- There is a continuing policing purpose for holding the record;
- The record is adequate, up to date and not excessive;
- That all personal records comply with the principles of the Data Protection Act 1998;
- The assessment as to the level of risk the person is perceived to present is correct.

7.3.2 Retention

The continued storage of and controlled access to information held for a policing purpose, which has been justified through the evaluation and review process.

7.3.3 Disposal

The removal of information from all police systems to the extent that the information cannot be restored. It must be justified through the evaluation and review process. See **7.8 Disposal** for further explanation.

7.4 National Retention Assessment Criteria

This subsection sets out the framework for decision making on the retention of police information. The key points relating to the National Retention Assessment Criteria are:

- The infringement of an individual's privacy created by the retention of their personal information must satisfy the proportionality test;
- Forces should be confident that any records they dispose of are no longer necessary for policing purposes;
- There should be a consistent approach to the retention of police information.

All records which are accurate, adequate, up to date and necessary for policing purposes will be held for a minimum of six years from the date of creation. This six-year minimum helps to ensure that forces have sufficient information to identify offending patterns over time, and helps guard against individuals' efforts to avoid detection for lengthy periods.

Beyond the six-year period, there is a requirement to review whether it is still necessary to keep the record for a policing purpose. The review process specifies that forces may retain records only for as long as they are necessary. The template in **Appendix 4** provides guidance on establishing whether or not information is still needed for a policing purpose.

The national retention 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. These questions are:

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. For example, while the theft of women's underwear falls in the category of property crime, such offences may indicate that the perpetrator carries a risk of committing sexual or violent offences.

Other 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.

Are there any concerns in relation to children or vulnerable adults?

In most cases behaviour brought to the attention of the police will be viewed much more seriously if the intended victim is a child or vulnerable adult. Any offence directed at a child or vulnerable adult could indicate a capacity for inflicting harm and the perpetrator, whether convicted or alleged, would need to be managed accordingly.

It is important that records relating to offences against children and vulnerable adults are retained, as they may later contribute to vetting and barring decisions for individuals who apply to work with these groups.

Did the behaviour involve a breach of trust?

A willingness to betray others, especially those in a position of vulnerability or 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. For example, an allegation of stealing from a department store would not necessarily lead to a prohibition on working with vulnerable people but an allegation of theft specifically targeted against an elderly person may do so.

Is there evidence of established links or associations which might increase the risk of harm?

Research in the area of criminal lifestyle and associations has demonstrated a clear link between spending time with other offenders and the likelihood of reoffending. This is particularly significant in circumstances where the identified group of offenders is already deemed to pose a risk of serious harm. For example, members of armed gangs, networks of paedophiles or organised crime syndicates may have greater opportunity or motivation to offend and can be affected by their peer group. This risk category includes members of organised crime groups, such as drug trafficking syndicates, whose criminal associates are integral to their offending.

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 resetting their clear period prior to a scheduled review. For example, a conviction for drink-driving may reset the clear period for a violent offender if alcohol is an identified risk factor which increases his or her risk of harm.

See **7.6.5 Clear Periods** for the definition and further detail of clear period.

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.

Concerns in this area may include symptoms of mental illness, obsessive or compulsive behaviour, paranoia or a serious lack of self-control.

Where the answer to any one of the questions above is 'Yes' then information relating to the individual being assessed should be retained and reviewed again at intervals designated by the review schedule given in **Appendix 4.** This ongoing review process will ensure that records remain adequate and up to date and that new information can be considered in the decision to retain records relating to individuals. The review will need to specifically consider whether the risk factors described here are still relevant. For example, concerns in relation to substance misuse or criminal associates may disappear over time and this should be taken into account in future reviews.

When used nationally, this method of assessment will ensure consistency across forces with regard to the type of information retained for designated time periods.

A completed copy of this assessment template should be kept on file as a record that the review has taken place and to support the subsequent decision. See **7.6.6 Audit and Supervision** for guidance on how to record the review process for audit purposes.

There may be other circumstances not covered by the criteria listed above, where forces consider that they have a genuine need to retain records. Wherever a record is assessed as being necessary and proportionate to the purpose it serves, it can be retained. For example, records of significant legal or historical interest or records relating to individuals who cause concern for reasons not listed in this assessment template can still be retained at force discretion.

Checklist 4

National Retention Assessment Criteria

- The following risk factors can be used to assess whether an individual poses a risk of harm, and information relating to him or her should continue to be retained for a policing purpose:
- Is there evidence of a capacity to inflict serious harm?
- Are there concerns in relation to children or vulnerable adults?
- Did the behaviour involve a breach of trust?
- Is there evidence of established links or associations with others which might increase the risk of harm?
- Are there concerns in relation to drug or alcohol misuse?
- Are there concerns that the individual's mental state might exacerbate risk?

7.5 Historical Data

Historical data is anything that was recorded prior to the date that the first edition of this guidance came into effect (1 April 2006). Key points to consider in relation to the review, retention and disposal of historical data are:

- Forces should review historical records when the subject of those records comes to police attention;
- Resources dedicated to reviewing other historical records should focus on information relating to certain public protection matters and other sexual, violent or serious offending.

Historical records which are reviewed when an individual next comes to the attention of the police are called Triggered Reviews. See **7.6.2 Triggered Reviews.**

During a triggered review, in addition to ensuring the adequacy and necessity of information being held on such a subject, forces will convert any related, unstructured or paper records into a searchable and accessible format and mark them in accordance with the government protective marking scheme (GPMS).

7.6 Review

The key points to consider in relation to the review of police information are:

- All necessary, adequate and up-to-date person records, regardless of type or classification, will be held for a minimum of six years;
- There is a presumption in favour of the retention of police information provided that it is not excessive, is necessary for a policing purpose, is adequate for that purpose and is up to date;
- Wherever an individual is believed to pose a high risk of harm, information about them will be retained for a further period specified by the Review Schedule.

The review process, as outlined in this subsection, is a full person record review. It focuses on an individual and any other records linked to them including other people, objects, location and events. Forces will review person records regularly throughout their lifetime to ensure that they are:

- **Necessary** – the record should hold some value for the Police Service in their effort to fulfil a policing purpose. 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 reoffending.

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. 'Necessary' in these cases should be determined by using the National Retention Assessment Criteria explained in **7.4 National Retention Assessment Criteria.**

It may also be necessary to retain records of particular legal or historical significance, or records relating to individuals who cause concern for reasons not listed in the National Retention Assessment Criteria. Forces have the discretion to decide which records they need beyond those specifically covered by this guidance.

- **Adequate** – in order to justify the retention of records they should be as complete as possible. Forces should make reasonable effort to collect enough information to allow them to identify every person, object, location and event as unique, see **4.5 Person Records.**

- **Accurate and up to date** – all record details should be accurate. Records should be updated with any new information.

- **Not excessive** – the amount and type of information held in relation to a person should be proportionate to the threat that they pose to others and the community. For example, the reclassification of offences over time may result in forces holding information in relation to offences that have subsequently been decriminalised. The test for justifying the retention of these records would be higher than for behaviour which remains illegal.

- **Data Protection Act Compliant** – any records of personal or sensitive personal data should also comply with the principles of the Data Protection Act 1998.

All person records held by the Police Service will be subject to:

- An initial evaluation in line with **5 Evaluation and Actioning of Police Information;**
- Any necessary triggered reviews;
- Scheduled reviews as specified in **Appendix 4.**

7.6.1 Initial Review and Evaluation

The initial stage of review of police information will be conducted at the point of input. The initial review process should ensure that records comply with the principles outlined in **5 Evaluation and Actioning of Police Information.**

The initial review and evaluation should also be used as an opportunity to provide feedback to staff about their record creation skills if necessary.

7.6.2 Triggered Reviews

Wherever further police information is submitted on an individual which relates to certain public protection matters or other sexual, violent or serious offending (Groups 1 and 2 see **7.6.3 Scheduled Reviews**), or the risk thereof, or relates to a person previously identified as presenting such a risk, a review should be conducted in relation to all police information held on that person.

Information which indicates risk to children or vulnerable adults should receive particular attention.

The policy for triggered reviews in each force should be published and clearly communicated to all staff to ensure understanding and adherence across the organisation.

Any related information contained within a person record that is no longer necessary for a policing purpose must be disposed of. Any records that are found to be inaccurate must be updated. In the event that a record is inaccurate beyond alteration it must be disposed of. For example, an individual may have accidentally, or through confusion, been linked to an address that they have never actually been associated with, and there is no policing purpose for having a record of it. Such a record is inaccurate beyond alteration and must be disposed of.

There is a significant difference between records that were once correct and inaccurate records that were never correct. For example, an offender may change address, vehicle or contact number and it is essential that a current record of these details is made. The offender's previous details should not, however, be deleted from the system. Previous addresses, vehicles or contact numbers are relevant to an offender's history and may in the future be relevant to further investigation into, for example, previously undetected offences or proceeds of crime recovery.

Any person record that is more than ten years old (Group 2), or six years (Group 3) see **7.6.3 Scheduled Reviews,** and is triggered for a review, should be risk assessed using the established National Retention Assessment Criteria (NRAC) detailed in **Appendix 4** and **7.4 National Retention Assessment Criteria.** If it is concluded that the subject in question continues to pose a high risk of harm, the record should be retained and reviewed again at intervals specified in the Review Schedule detailed in **Appendix 4.**

Triggered reviews should also be held in the following circumstances:

- **Statutory disclosures** – this includes disclosures to the Independent Safeguarding Authority (ISA), Department of Children Schools and Families (DCSF) and Department for Innovation Universities and Skills (DIUS) vetting and barring schemes. It is essential that the information being disclosed is correct and relevant to the matter in question. Further details of the CRB relevancy test can be found in section **6 Information Sharing.**

- **Requests for information made by other law enforcement agencies** – person records shared with other law enforcement agencies should be reviewed for their accuracy, adequacy and necessity. Forces should ensure that only the most current and accurate record is shared and that the test of proportionality has been applied.

- **Subject Access Requests** – subject access requests should be used as a trigger for review. Forces must disclose the information available at the time of the request and only update or dispose of records once the request has been responded to.

Routine amendments or disposals that would have been made regardless of the request, as covered by section 8.6 of the Data Protection Act 1998, should still be made.

Note: By the time a review is triggered, the information being reviewed may have already been used to make decisions and justify police action. Consequently, any updates must be adequately documented for audit purposes. For further detail on the audit requirements of the reviewing process, see **7.6.6 Audit and Supervision.**

7.6.3 Scheduled Reviews

The Review Schedule in **Appendix 4** of this guidance 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 whose criminal activity is lower level but higher in frequency also pose a risk of harm to the public. Information about them should, therefore, be retained on police systems for as long as they continue to engage in criminal activity. The use of designated clear periods prevents forces from having to justify the continued retention of information related to prolific offenders for as long as they continue to offend. For the purpose of this guidance, 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 suspected offender for behaviour that can be considered a relevant risk factor. The triggered review process will ensure that records relating to prolific offenders remain adequate and up to date.

The Review Schedule is offender focused rather than focused on business areas. It is based on the following three premises:

1. Past behaviour is an indicator of future behaviour and the type of offence an individual is involved in, or alleged to be involved in, is a clear indicator of risk;

2. Information relating to those offenders who pose the highest risk of harm to the community must be retained the longest;

3. Where a person record is linked to multiple offences, the most serious offence will determine the review category for all of the offences.

The Police National Legal Database has been updated to show a MoPI review group for each offence. A comprehensive list has been supplied to all forces and will be regularly updated allowing forces to search by offence, offence code and MoPI review group.

For audit purposes, a record must be kept of every review undertaken, irrespective of whether it resulted in any alterations or disposal. For guidance on how to record the review process for audit purposes, see **7.6.6 Audit and Supervision.**

Under the Review Schedule, information held for policing purposes is divided into four groups.

Group 1: Certain Public Protection Matters

The ***MoPI Code of Practice*** acknowledges 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 policing purposes.

Certain public protection matters are defined fully in **2.3 Critical Information Areas.** They are:

- Information relating to all offenders who have ever been managed under MAPPA;
- Information relating to individuals who have been convicted, acquitted, charged, arrested, questioned or implicated in relation to murder or a serious offence as specified in the Criminal Justice Act 2003 (CJA) or historical offences that would be charged as such if committed today;
- Potentially dangerous people.

Forces must retain all information relating to certain public protection matters until such time as a subject is deemed to have reached 100 years of age (this should be calculated using the subject's date of birth). There is still a requirement, however, to review this information regularly to ensure that it is adequate and up to date. This must be done every ten years. See **7.7.2 Which Records Should Not Necessarily Be Retained** for advice on duplicate records.

Due to the seriousness of this group, no distinction is made between the type or classification of information that can be retained for 100 years; information retained under this grouping can include intelligence of any grading.

There may be extreme cases where the retention of records relating to certain public protection matters would be disproportionately injurious to the individual they are recorded against. For example, an individual arrested on suspicion of murder for a death that is subsequently found to have been the result of natural causes, or an entirely malicious accusation that has been proved as such, would both generate records that can only be adequate and up to date if they reflect what actually happened. Particular care must be exercised in disclosing any such records to avoid any unnecessary damage to the person who is the subject of the record.

Additionally, offences that have been amended by more recent (CJA) legislation and are now considered serious specified offences under the CJA should be retained as part of this group. For example, under the Sexual Offences Act 1956 the offence of Unlawful Sexual Intercourse with a girl aged 13–16 years attracted a maximum sentence of two years' imprisonment. Under the Sexual Offences Act 2003 this offence, now called sexual activity with a child, carries a maximum sentence of fourteen years' imprisonment and is listed as a 'serious specified offence' under the CJA. For the purposes of this review and retention process, individuals dealt with under the Sexual Offences Act 1956 should have their records retained as though the offence or alleged offence occurred recently.

Group 2: Other Sexual, Violent or Serious Offences

For the purpose of this guidance, a sexual offence is any listed in Schedule 3 of the Sexual Offences Act 2003. A violent offence is any of those specified as such in the current Home Office Counting Rules for recorded crime. A serious offence is any offence shown as such on the Police National Legal Database (PNLD). This group also includes all specified offences that are not serious offences as defined in the CJA. A full list of these offences is recorded on the PNLD.

Information relating to sexual, violent or serious offences that are not listed as serious specified offences in the CJA can only be retained for as long as the offender or suspected offender continues to be assessed as posing a risk of harm, using the NRAC in **Appendix 4.**

After every ten-year clear period, these records should be reviewed and a risk-based decision made as to whether they should be retained or disposed of. This group includes any information related to persons convicted, acquitted, charged, arrested, questioned or implicated with an offence within this group. If the individual in question continues to offend or is implicated in continued offending then records relating to them must be retained. In these circumstances, however, the absence of a clear period will mean that forces do not have to conduct a scheduled review or justify the continued retention of such records. The triggered review process will ensure that records relating to this group of offenders remain adequate and up to date.

Group 3: All Other Offences

Records relating to people who are convicted, acquitted, charged, arrested, questioned or implicated for offending behaviour which does not fall within Group 1 or Group 2 are dealt with in Group 3.

Records that fall within this group do not necessarily have to be reviewed. Forces may opt to use a system of time-based, automatic disposal for classes of information in this group if it is considered that the risk of disposing of these records is outweighed by the administrative burden of reviewing them or the cost of retaining them.

Forces who opt to use time-based disposal for all or a proportion of their Group 3 records must observe the following principles:

- The criteria by which forces decide which Group 3 records to review and which to automatically dispose of must be outlined in the Information Management Strategy (IMS);
- The risk of disposing of records without review lies with the chief officer;
- All records subject to time-based disposal must still be retained for an initial six-year period;
- Forces must have a mechanism for identifying those Group 3 individuals who continue to reoffend or who are implicated or suspected of being implicated in offending, and retain records relating to them;
- Forces must have a mechanism for identifying those individuals who have demonstrated a capacity for inflicting serious harm, using the NRAC in **Appendix 4** and flagging records relating to them for an Exception Review, see **7.6.4 Exception Reviews;**
- Any Group 3 records that forces wish to retain for longer than six years must be reviewed at five-yearly intervals and risk assessed using the NRAC in **Appendix 4.**

Group 4: Miscellaneous

- Undetected Crime

  Records relating to undetected Group 1 offences should be retained for a minimum of 100 years from the date reported to the police.

  Other records of undetected offences should be retained for a minimum of six years from the date reported to the police. Forces should be mindful that these are minimum periods; they may keep undetected crime records for longer if they feel it necessary. There are no additional requirements to review these records above and beyond the requirements imposed by relevant investigative guidelines.

- CRB Disclosures

  The CRB Quality Assurance Framework states that information disclosed to the CRB under the Police Act 1997 for vetting purposes should be retained for ten years.

  Again, these packages of information will be a copy of the original record. Provided there is no subsequent ongoing legal action relating to such a disclosure, these records can be disposed of after ten years.

- Intelligence Products

  Intelligence products used to support police inquiries or investigations will often be linked to a person record and should be reviewed in accordance with the Review Schedule shown in **Appendix 4.** The type of criminal activity being examined determines the length of time between reviews.

- Missing Persons

  In accordance with ***ACPO (2010) Guidance on the Management, Recording and Investigation of Missing Persons*, Second Edition** information relating to open missing persons cases should be retained until the person is located. There are no additional requirements to review outstanding missing persons cases beyond those outlined in that guidance.

  For cases of missing persons who have subsequently been located safe and well, information should be retained for a minimum of six years. If this initial six-year period is clear, ie, the individual does not go missing again and there are no subsequent indications of abuse, domestic violence or other factors that might place the individual at risk, the record should be disposed of.

- Victim and Witness Information

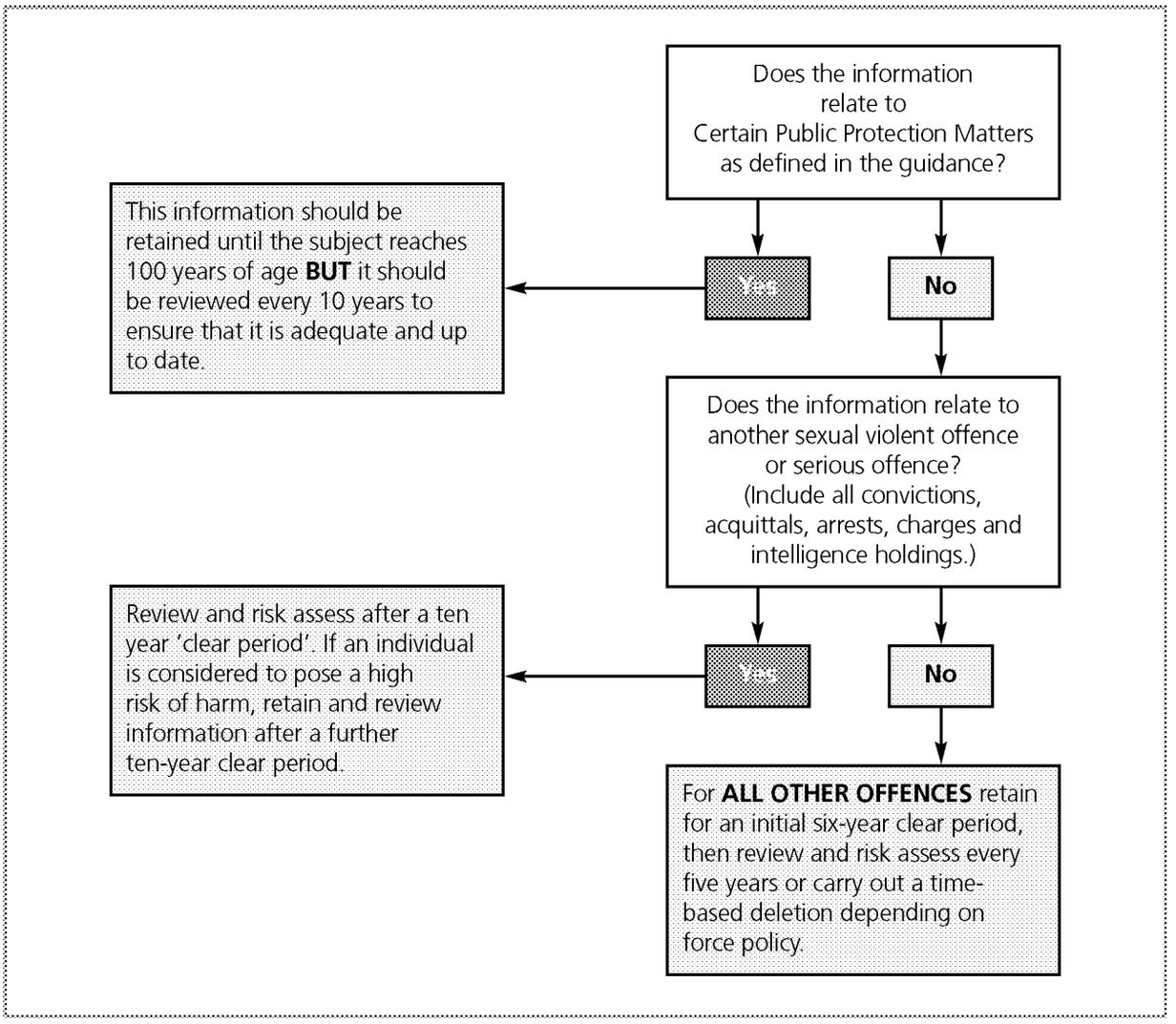
  Records relating to the victim of an offence and any witnesses should be retained for an initial six-year clear period or for the length of time required by the CPIA if this is longer. See **7.2.3 Criminal Procedure and Investigations Act 1996** for a brief description of the CPIA requirements; refer to section 5 of the CPIA Code for more detail.

Beyond this point, the decision about whether to retain victim and witness details should be made on a case-by-case basis. Records should be retained if they provide detail of an offender's MO or relevant risk factors. Witness statements will generally fall into this category, see **7.7.1 The Decision To Retain.** If, however, this detail is duplicated elsewhere, consideration can be given to deleting victim and witness information from the system.

In all cases victim and witness details should be handled with care and in accordance with their right to privacy.

In circumstances where a victim or witness is recorded on police systems as an offender or suspect in another matter, their details should be retained and reviewed in accordance with the incident in which they are the person of interest.

Figure 2 – Information Review Schedule Process Chart



7.6.4 Exception Reviews

Under this guidance forces are able to opt for a system of time-based disposal for records that relate to Group 3 offences, as defined in **7.6.3 Scheduled Reviews.** If, however, an offender or suspected offender's behaviour suggests that they may pose a high risk of harm to others, forces must have a mechanism in place for highlighting the relevant person records for an exception review, instead of disposing of them automatically.

For the purpose of determining whether an individual who has been accused, suspected, arrested, charged, convicted or acquitted of a Group 3 offence poses a high risk of harm, forces should use the criteria outlined in the NRAC. See **7.4 National Retention Assessment Criteria.**

If, however, any of the risk factors listed below are present, the relevant person records must be directed into the review process:

- Is there evidence of a capacity to inflict serious harm?
- Are there concerns in relation to children or vulnerable adults?
- Did the behaviour involve a breach of trust?
- Is there evidence of established links or associations which might increase the risk of harm?
- Are there concerns in relation to substance misuse?
- Are there concerns that the individual's mental state might exacerbate risk?

The task of highlighting records for an exception review is one that should be done at the point of record creation.

7.6.5 Clear Periods

The definition of a clear period used in this guidance is different from that used in the ***PNC Retention Guideline.***

The Review Schedule in **Appendix 4** states that reviews take place after designated clear periods. If a subject last came to the attention of the police through an intelligence report that did not lead to any police action, the clear period will begin on the date that the report was submitted.

Where the relevant behaviour led to police action, such as arrest, questioning or any further enquiries, the clear period will begin on the date of the last action. In cases where a fixed penalty notice or caution was issued the individual's clear period will begin on the date of issue.

Where a person is charged with an offence but the case is either not proceeded with or a court acquits them, the clear period will begin on the date the decision was taken or handed down.

If the individual's last relevant contact with the criminal justice system was by way of a court ordered sentence, the clear period will begin when that sentence has expired completely. In the case of custodial sentences this includes any period served on licence in the community, following the custodial element of the sentence.

Further behaviour brought to the attention of the police and which indicates a relevant risk of harm will reset an individual's clear period. The relevance of such behaviour must be determined on a case-by-case basis. For example, a new charge of driving under the influence of alcohol might not be relevant in the case of all sex offenders. If, however, an individual's history suggests that alcohol misuse is a pre-cursor to offending, this would be relevant and should be used to reset their clear period.

Behaviour which can lead to a clear period being reset does not necessarily have to be a new offence or suspected offence, but it must be evidence of a risk of harm to others.

An individual's clear period is also reset by a request for information made by other law enforcement agencies and by requests for CRB disclosure. Clear periods **are not** reset by subject access requests.

7.6.6 Audit and Supervision

The key points to consider for the audit and supervision of the review process are:

- All triggered, scheduled and exception reviews of police records must be documented, regardless of whether they result in any change;
- The IMS should specify the level at which decisions to dispose of records relating to sexual, violent and serious offences (Group 2) are taken;
- The IMS should specify an inspection of a sample of force records every twelve months.

Documenting the Review Process

The NRAC in **Appendix 4** has been designed in a table format to assist forces with the requirement to record reviews and any subsequent decisions to retain information.

When conducting a review, 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 NRAC form should be completed. It should then be stored either electronically or in hard copy on the relevant file.

Any system-generated records created to document a review must log the date of review, the reviewer's name, the outcome and the reason for the decision taken.

In complex cases, where the review process takes several days, a time period can be recorded as the date of review.

In the case of triggered reviews, the reviewing officer must provide an explanation of how and why the triggered review came about.

The retention assessment criteria section of this 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 records 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 record is not created to document a review and the reviewing officer is relying on the NRAC form, 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.

Authorising the Review Process

All reviews that result in a decision to dispose of a record or change its category should be authorised by the reviewing officer's line manager. Forces may require line mangers to authorise other reviews if they wish. The NRAC form includes a space for their authorisation.

The decision to retain information can be approved by a line manager at any level.

For offences that fall within Group 2 – other sexual, violent or serious offences (see **7.6.3 Scheduled Reviews**) there is a presumption in favour of retention, and the decision to dispose of any records from this group, therefore, requires authorisation. The IMS will specify an appropriate level for this decision to be taken within the force.

Where forces have opted to review the Group 3 – any other offence records they hold, decisions to retain or dispose can be approved by the reviewing officer's line manager. See **7.6.3 Scheduled Reviews.**

The time-based disposal of Group 3 records does not require any further authorisation beyond that already given by a chief officer in his/her decision to take this option. This approach should be specified in the IMS.

Annual Inspections and Monthly Audits

To ensure the quality of review processes, forces will set out in an IMS the process for overseeing annual inspections of a sample of force person records. This is to ensure that they are Data Protection Act compliant and being reviewed in accordance with this guidance.

These inspections must be carried out independently of staff in the business area where the records are held.

Additionally, local managers should, in line with the IMS, undertake regular quality assurance audits of information held by their unit or business area.

7.7 Retention

The key points to consider in relation to the retention of police information are:

- When the decision is made to retain information about a person, consideration should be given as to whether every individual record needs to be retained;
- Information that is to be retained must be managed in accordance with ***ACPO/ACPOS (2002) Information Systems Community Security Policy;***
- Information that is to be retained must be both searchable and retrievable by staff who are appropriately vetted and have a need to know.

The retention of information relating to criminal activity and known and suspected offenders allows the Police Service to develop a more proactive approach to policing. By contributing to the identification of criminal patterns and threats and helping to prioritise the subsequent deployment of policing resources, information retention assists forces to prevent and detect crime and protect the public. It is, however, impractical and unlawful for forces to retain every piece of information collected. Consideration must, therefore, be given to the types of information that need to be retained and the practical implications of storing these records in their various formats.

7.7.1 The Decision To Retain

Scheduled reviews require the reviewing officer to conduct an assessment of the risk of harm posed by the subject of the information under review. See **7.6.3 Scheduled Reviews.**

If the individual under review meets any of the criteria outlined in the National Retention Assessment Criteria (NRAC) (see **Appendix 4**) then the retention of records relating to them is proportionate to the level and type of risk they pose. Hence, these records must be retained and reviewed again at a later date specified in the Review Schedule in **Appendix 4.**

In those circumstances where individual records cannot be separated out, for example, police pocket notebooks, the entire collection of records should be retained according to the most serious offence they contain. In the case of pocket notebooks and similar documents, relevant police information should be transferred to a primary business area as soon as is practicable.

It should be noted that a decision to retain records relating to a particular individual does not necessarily mean that every piece of information held in relation to them needs to be kept. The reviewing officer should use their discretion to identify those records that contain sufficient information to contribute to understanding the nature of the offence or the type of risk posed.

Similarly, any records that do not contain sufficient detail to identify the circumstances of the offence are not adequate for purpose and cannot be retained.

7.7.2 Which Records Should Not Necessarily Be Retained

During an investigation, a number of pieces of information will have been collected for purely administrative purposes and do not have any independent significance. It is not necessary to keep these ancillary records as part of a file that has been marked for retention as they do not contribute to understanding the nature of the offence or the type of risk posed.

Information that is duplicated across force systems should also be minimised. Consideration should be given to the amount and type of detail held on individual systems and the extent to which this is duplicated in others, with a view to disposing of those that are surplus to requirements. It may also be more practical to retain electronic records than paper ones and, provided that the reviewing officer is satisfied that the relevant information contained in paper records is also held electronically in a searchable format, the paper records can be destroyed.

Original exhibits do not need to be retained in circumstances where it is unreasonable to do so, however, a copy should be stored in the form of photographs, video recordings or digital images.

Special care needs to be taken when deciding whether to keep intelligence products. Although intelligence products are generally based on information already held on police systems, they often present this information in a more concise and helpful format. It may, therefore, be useful to keep them. If, however, they duplicate information on other systems and do not add any value, then they can be disposed of.

7.7.3 Storage

The methods for storing records of police information will depend on whether they carry a protective marking. ***Cabinet Office (n.d.) Government Manual of Protective Security*** and ***ACPO/ACPOS (2002) Information Systems Community Security Policy*** specify requirements for storing classified material. All forces must develop and implement a policy for disposing of records in accordance with these standards.

7.7.4 Access and Retrieval

Records that have been marked for retention must be stored in a format and location that allows them to be searched and retrieved.

Police information can only be accessed for authorised policing purposes, and force policy must ensure that only those staff who are vetted accordingly and who have a legitimate need to know are permitted access to protectively marked information.

All employees, including contract staff, are personally responsible for ensuring that they have access to and fully understand and comply with all relevant force security policies and operating procedures. It is the supervisor's duty to ensure that all users of information systems are aware of these policies and procedures and adhere to them.

7.7.5 Archiving

The use of archives to store records and limit access to them is an option for forces, and a decision should be made on a force-by-force basis. It must be emphasised, however, that archiving is a form of retention and is not to be used for information that must be disposed of.

7.7.6 Audit and Supervision

All reviews that result in a decision to retain records must be recorded on the form held in **Appendix 4.** Full details on recording the reviewing process for audit purposes can be found in **7.6.6 Audit and Supervision.**

7.8 Disposal

For the purpose of this guidance, disposal is the removal of information from all police systems, justified through the review process, to the extent that it cannot be restored.

The key points to consider in relation to the disposal of police information are:

- Disposal means removal of information from all police systems;
- The IMS, or its supporting documentation, will set out who can authorise the disposal of police records;
- Information must be disposed of in accordance with ***ACPO/ACPOS (2002) Information Systems Community Security Policy.***

Information is disposed of and removed from police systems 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 details of a record marked for disposal do not continue to exist on any police systems, including paper or other copies or within other documentation such as intelligence products.

7.8.1 The Decision To Dispose of Information

Where a scheduled review has taken place after a designated clear period, and the completed NRAC does not indicate that the subject continues to pose a risk of harm, the record under review must be disposed of.

7.8.2 Secure Disposal

The method of disposal for records of police information will depend on whether they carry a protective marking. ***Cabinet Office (n.d.) Government Manual of Protective Security*** and ***ACPO/ACPOS (2002) Information Systems Community Security Policy*** specify requirements for the handling and disposal of classified material. All forces must develop and implement a policy for disposing of records in accordance with these schemes.

7.8.3 Archiving

Records that have been marked for disposal because they are inadequate or are no longer necessary cannot be archived. Archiving is a form of retention and should only be used as a means of restricting access to those records that can continue to be held lawfully. See **7.7.5 Archiving.**

Records which no longer have a policing purpose but which may have historical or academic value may be archived for long-term retention outside the operational environment. It must be clear that the records are kept for this purpose only.

7.8.4 Audit

The template provided in **Appendix 4** must be completed for all reviews where circumstances do not allow for a system-generated record to be created. This form must also be presented to the authorising officer for their approval and signature.

In cases where a record has been marked for disposal it is not, however, appropriate to retain the completed risk assessment form for audit purposes, as this will contain some detail of the record and undermine the attempt to remove this detail from police systems. The IMS will specify that a disposal schedule is maintained containing the following information:

- Date of decision;
- Number of records;
- Whether the records were considered inadequate or no longer necessary for a policing purpose.

Under no circumstances should records documenting a decision to dispose of information hold the personal details of individuals. The review process outlined in this guidance will ensure that forces can justify the disposal of information. Once a record is considered to be either inadequate or no longer necessary, there is no reason why a force should have any indication they ever had it.

7.9 Responsibilities

7.9.1 Managers

- Ensure that the IMS sets out a process for reviewing records in accordance with this guidance;
- Decide at what level decisions to retain and dispose of records can be taken;
- Ensure a dip sample of records held by their department is undertaken;
- Ensure staff responsible for undertaking reviews are trained in accordance with the National Training and Delivery Strategy.

7.9.2 Supervisors

- Authorise the outcome of all reviews conducted in their area of responsibility;
- Ensure that the review policy in the IMS is followed;
- Provide feedback to staff;
- Ensure users of systems are aware of and adhere to force policies and procedures relating to information management and systems.

7.9.3 Users

- Follow this guidance for reviewing records;
- Access, understand and follow force security policies and operating procedures;
- Establish and enter the review date for a record at the point of creation;
- Follow the NRAC in **Appendix 4** when reviewing records to determine their continued necessity for a policing purpose;.
- Document the review process using the form in **Appendix 4** wherever there is no automated mechanism in place;
- Ensure that information to be disposed of is not duplicated and, therefore, retained elsewhere.

Appendix 1

Code of Practice on the Management of Police Information

The *MoPI Code of Practice* makes reference to organisations which no longer exist. It has not been necessary to update the code and lay it before parliament again as it applies to successor organisations.

Code of Practice on the Management of Police Information

Made by the Secretary of State for the Home Department

under

sections 39 and 39A of the Police Act 1996

and

sections 28, 28A, 73 and 73A of the Police Act 1997

Prepared by: The National Centre for Policing Excellence

July 2005

Contents

1 Introduction

1.1 Purpose of the code

1.1.1 Police forces have a duty to obtain and use a wide variety of information (including personal information), in order to discharge their responsibilities effectively. They need the support and cooperation of the public in doing so. The purpose of this code and associated guidance is to assist the police to carry out that duty.

1.1.2 The responsibility for the management and use of information within the Police Service rests with the chief officer of the police force which owns the information.

1.1.3 Chief officers of police must therefore ensure that their forces adopt practices for the management of information that ensure such information is used effectively for police purposes and in compliance with the law.

1.1.4 The purpose of this code is to ensure that there is broad consistency between forces in the way information is managed within the law, to ensure effective use of available information within and between individual police forces and other agencies, and to provide fair treatment to members of the public.

1.1.5 This code sets out the principles governing the management of information (including personal information) which the Police Service may need to manage and use including:

a) procedures to be applied in obtaining and recording that information;
b) procedures to ensure the accuracy of information managed by the police;
c) procedures for reviewing the need to retain information and, where it is no longer needed, to destroy it;
d) procedures governing authorised sharing of information within the Police Service and with other agencies; and
e) measures to maintain consistent procedures for the management of information within all police forces so as to facilitate information sharing and the development of service-wide technological support for information management.

1.1.6 In doing so, it recognises that effective use of information for police purposes requires consistent procedures to be in place throughout the Police Service.

1.1.7 The procedures and equipment to give effect to the principles set out in this code may change. This code will therefore be supported by more detailed and extensive guidance that will define information management standards required within forces. That guidance may change from time to time, but must be framed in compliance with the principles established by this code.

1.2 Statutory basis of the code

1.2.1 This code of practice comes into effect on 14 November 2005.

1.2.2 Nothing in this code alters the existing legal powers or responsibilities of any police authority, chief officer of police, or other person.

1.2.3 This code of practice is made under:

a) section 39 of the Police Act 1996, which permits the Secretary of State to issue codes of practice relating to the discharge by police authorities of any of their functions;
b) section 39A of the same Act, which permits the Secretary of State to issue codes of practice relating to the discharge of their functions by chief officers where it is necessary to do so for the purpose of promoting the efficiency and effectiveness of police forces in England and Wales;
c) section 28 of the Police Act 1997, which permits the Secretary of State to issue codes of practice relating to the discharge by the National Criminal Intelligence Service (NCIS) Service Authority of any of its functions;
d) section 73 of the Police Act 1997, which permits the Secretary of State to issue codes of practice relating to the discharge by the National Crime Squad (NCS) Service Authority of any of its functions;
e) section 28A of the Police Act 1997, which permits the Secretary of State to issue codes of practice relating to the discharge by the Director General of the NCIS of any of his functions; and
f) section 73A of the Police Act 1997, which permits the Secretary of State to issue codes of practice relating to the discharge by the Director General of the NCS of any of his functions.

1.2.4 This code recognises that there is an existing legal framework for the management of information in legislation relating to data protection, human rights and freedom of information.

1.2.5 It applies directly to the police forces maintained for the police areas of England and Wales defined in section 1 of the Police Act 1996, and to the NCS and the NCIS.

1.2.6 It is available for adoption by other agencies including other police forces not covered by section 1 of the 1996 Act and law enforcement agencies within the United Kingdom that exchange information with the Police Service in England and Wales.

1.2.7 References in this code to chief officers of police apply, in the case of NCS and NCIS, to the Directors General of those organisations.

1.3 Role of HM Inspectors of Constabulary

1.3.1 HM Inspectors of Constabulary will monitor police forces' compliance with this code, associated guidance, and standards.

1.4 Role of the Central Police Training and Development Authority

1.4.1 The Central Police Training and Development Authority (CPTDA), or any successor body designated by the Secretary of State, has responsibility on behalf of the police forces of England and Wales for the development of guidance under this code. Such guidance and any subsequent amendments will be prepared in consultation with the Association of Chief Police Officers, the Association of Police Authorities, and such other persons as the CPTDA thinks fit.

1.5 Consultation

1.5.1 Consultation has been carried out by the CPTDA in accordance with the statutory provisions.

2 The Management of Information for Police Purposes

2.1 The management of police information

2.1.1 In this code, references to the management of police information include the processes of obtaining, recording, storing, reviewing, deleting and sharing information, including personal information, for police purposes in accordance with principles governing those processes set out at **4** below.

2.2 Information for police purposes

2.2.1 In this code references to information include data. All information, including intelligence and personal data obtained and recorded for police purposes, is referred to as police information.

2.2.2 For the purposes of this code, police purposes are:

a) protecting life and property;
b) preserving order;
c) preventing the commission of offences;
d) bringing offenders to justice; and
e) any duty or responsibility of the police arising from common or statute law.

3 A National Framework for the Management of Police Information

3.1 National guidance on management of police information

3.1.1 Guidance under this code will:

a) set out the strategic information needs of the Police Service in line with the National Intelligence Model;
b) direct the management of police information within police forces so as to ensure consistent procedures throughout the Police Service for obtaining, recording, storing, reviewing, deleting and sharing information; and
c) identify the minimum standards required within police forces to provide a standard basis for common police IT systems for the management of police information.

3.2 An Information Management Strategy to be applied within each police force

3.2.1 Chief officers will establish and maintain within their forces an Information Management Strategy, under the direction of an officer of ACPO rank or equivalent, complying with guidance and standards to be issued under this code unless that guidance is superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996.

3.3 National system requirements for the management of police information

3.3.1 For the purpose of achieving throughout the Police Service the standards described at **3.1.1**.above, guidance issued under this code, unless superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996, may specify procedures to be adopted within police forces for the management of police information systems.

3.4 Security of police information

3.4.1 Chief officers should ensure that arrangements within their forces for managing police information include procedures and technical measures to prevent unauthorised or accidental access to, amendment of, or loss of police information. Such procedures should comply with guidance issued under this code unless superseded by regulations made by the Secretary of State under section 53 or section 53A of the Police Act 1996.

3.5 Training for staff engaged in police information management

3.5.1 Guidance issued under this code may identify key posts for the management of police information, and may specify the qualifications to be held by staff in those posts, and the training required for such staff.

3.5.2 Chief officers of police should arrange the selection and training of those to be appointed to such posts so as to ensure attainment of standards of competence.

3.5.3 Those attaining the required standards of competence for such posts will be entered on the relevant professional register. They will remain on the register provided their continued suitability and competence remain assured in accordance with provisions for re-assessment and re-qualification.

3.5.4 Training for these purposes is not only to ensure compliance with the legal framework for information management and the maintenance of high standards of competence, but also to ensure the consistency of police information management procedures throughout the Police Service.

3.5.5 The body responsible for the approval and accreditation of training courses and trainers for these purposes or any successor body will be designated by the Secretary of State. Training standards will be kept under review by the accreditation authority.

4 Key Principles Governing the Management of Police Information

4.1 Duty to obtain and manage information

4.1.1 Chief officers have a duty to obtain and manage information needed for the police purposes described at **2.2** above.

4.1.2 Chief officers must ensure that arrangements within their forces for the management of police information comply with the principles set out in the following paragraphs, and with guidance issued under this code to give effect to those principles.

4.2 Requirement for police information

4.2.1 Chief officers must ensure that arrangements to gather police information comply with the principles of the National Intelligence Model.

4.3 Grading and recording of police information

4.3.1 Information should be recorded where it is considered that it is necessary for a police purpose. Chief Officers must establish recording procedures in accordance with guidance issued under this code, which emphasise the need for information to be as complete and accurate as possible.

4.3.2 Where appropriate and in accordance with guidance to be issued under this code, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information should be recorded to permit later review, reassessment and audit.

4.3.3 Information should be assessed for reliability in accordance with guidance to be issued under this code.

4.3.4 The format in which the information is recorded should comply with standards agreed and applied across the Police Service by means of guidance issued under this code, to facilitate exchange of information and processing within standard police IT systems.

4.4 Ownership of police information

4.4.1 Chief officers of police are responsible for information originally recorded for police purposes by their forces. They or their successors in the force retain responsibility for subsequent reviews and decisions to retain or delete that information. The related responsibilities of those who may share that information are set out at **4.10** below.

4.5 Review of police information

4.5.1 Information originally recorded for police purposes must be reviewed at intervals to be prescribed in guidance under this code, which may prescribe different intervals for different categories of information.

4.5.2 At each review, the likelihood that the information will be used for police purposes should be taken into account. Chief officers should ensure that this process is audited.

4.6 Retention and deletion of police information

4.6.1 On each occasion when it is reviewed, information originally recorded for police purposes should be considered for retention or deletion in accordance with criteria set out in guidance under this code.

4.6.2 Guidance will acknowledge that there are certain public protection matters which are of such importance that information should only be deleted if:

a) the information has been shown to be inaccurate, in ways which cannot be dealt with by amending the record; or
b) it is no longer considered that the information is necessary for police purposes.

4.7 Sharing of police information within the UK Police Service

4.7.1 Guidance under this code may specify a protocol for sharing information.

4.7.2 Subject to any constraints arising from guidance based on section **4.9** below, the content and the assessment of the reliability of information recorded for police purposes should be made available to any other police force in England and Wales which requires the information for police purposes.

4.7.3 Subject to any constraints arising from guidance based on section **4.9** below, the same degree of access to information recorded for police purposes by police forces in England and Wales should be afforded to other police forces in the United Kingdom provided that the chief officer responsible for the record is satisfied that the police force seeking access to the information applies the principles set out in this code.

4.7.4 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 either:

a) by response to bilateral or multilateral requests for information to police forces; or
b) by holding such information on IT systems to which police forces referred to above may be given direct access.

4.8 Sharing of police information outside the UK Police Service

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

4.8.2 In addition, chief officers may arrange for other persons or bodies within the UK or overseas to receive police information where the chief officer is satisfied that it is reasonable and lawful to do so for the purposes set out at **2.2** above.
In deciding what is reasonable, chief officers must have regard to any guidance issued under this code.

4.8.3 The procedures for making such information available, and the extent to which it is made available, must comply with guidance to be made under this code, and with any protocol (whether at national or local level) which may be agreed with persons or bodies needing to receive such information.

4.8.4 In circumstances not covered by any such protocol, a chief officer may give access to police information in response to a request from any person or body to the extent that the chief officer believes this request to be lawful and reasonable for the purposes set out at **2.2** above, and in compliance with guidance issued under this code.

4.9 Protection of sensitive police information and sources

4.9.1 Guidance under this code may provide for special procedures to be applied to a request for access to information recorded for police purposes, in any case where it is necessary to protect the source of sensitive information or the procedures used to obtain it.

4.10 Obligations of those receiving police information

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

a) Police information made available in response to such a request should be used only for the purpose for which the request was made;
b) If other information available, at the time or later, to the person or body requesting police information tends to suggest that police information is inaccurate or incomplete, they should at the earliest possible moment inform the chief officer concerned of such inaccuracy or incompleteness, either directly or by reporting the details to the managers of the central police system through which the information was provided.

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

Appendix 2

5x5x5 Information/Intelligence Report

This appendix describes the process of how to record and evaluate information on the national Information/Intelligence report, commonly known as a 5x5x5. Initial risk assessment of received information is also discussed here.

Contents

1.1 5x5x5 Information/ Intelligence Report

Information to be considered for intelligence purposes may be recorded in a number of business areas, such as crime reports and custody records. The 5x5x5 is the format to record specific intelligence from these business areas and all other information to be considered for intelligence purposes.

The 5x5x5 is a tool which allows the Police Service to manage information which has risk attached to it. For example, the 5x5x5 can be used to assess the risk of exposure of the source or the use of the material and safeguard the source and the operation the information relates to. It is the standard format for managing the evaluation, the source and the provenance of the information and the manner in which it should be handled and disseminated. The use of a 5x5x5 is the start of the audit trail which is integral to the NIM process, and ensures consistency between forces and enables forces to share intelligence more easily.

Management of the 5x5x5 recording and evaluation process requires effective intelligence management processes as described by NIM to be in place. See ***ACPO(2005) Guidance on the National Intelligence Mode.***

1.2 What Is a 5x5x5?

The 5x5x5 is a national Information/Intelligence Report and comprises three forms.

Form A An Information/Intelligence Report which covers the three elements of:

- Source evaluation;
- Information/intelligence evaluation;
- Handling codes.

This form contains risk management processes.

Form B An Information/Intelligence Report continuation form.

Form C A further risk assessment process. This is a more comprehensive risk assessment record that is used in particular circumstances where the handling codes alone are not sufficient to manage the risk of dissemination of the information.

1.3 When Should a 5x5x5 Be Used?

The 5x5x5 should be used to record sensitive information for policing purposes, see **1.2 What is Police Information?** in the main body of this document. Examples of information appropriate to record on a 5x5x5 are:

- Information given to the police by a member of the public in confidence;
- Information from anonymous sources, for example, Crimestoppers or the anti-terrorism hotline;
- Information of a personal or confidential nature received from someone who has access to it because of their occupation, for example, hotel, airline, ticket office or currency exchange staff;
- Information from a covert human intelligence source (CHIS);
- Information obtained by covert means, for example, the product of technical or other surveillance activity;
- Information from other law enforcement agencies that is supplied in confidence, or is from a sensitive source (and would, therefore, be recorded on a 5x5x5 had it originated from the Police Service);
- Information from liaison with other partner agencies, for example, CRP, CDRP, YOT;
- Information obtained by police officers and staff in the course of their duties, for example, patrol officers, front desk staff, PCSOs and interviewing officers.

This list is not exhaustive.

The 5x5x5 should not generally be used when information is recorded in another business area, for example:

- Crime reports;
- Incident records;
- Custody records.

It may, however, also be appropriate to use a 5x5x5 in circumstances where business areas are not searchable through the intelligence system. Furthermore, the 5x5x5 may be used where it is necessary to record information from different business areas in order to make sense of a number of facts, highlighting a risk from, or to, a person. Further examples may include:

- The reasons for the revocation of a firearms licence;
- Details about a person who may be a risk to children or vulnerable adults;
- Details about a known or suspected domestic violence perpetrator;
- Allegations of threats to life or of serious harm;

- Details of potentially dangerous people who pose a threat to the public;
- Where it is necessary to restrict or control the subsequent dissemination of the information.

1.4 How to Complete the 5x5x5 (Forms A and B)

The 5x5x5 report contains basic details identifying the person completing and submitting the report. It will also contain the time and date of submission and the signature of the person submitting the report, if a paper copy is used. Many electronic systems for recording 5x5x5 reports include electronic identifiers and so do not require a signature.

An audit trail of the information recorded on the 5x5x5 is essential and all police staff **must** ensure that these details are completed.

The following sections outline each individual aspect of the 5x5x5 report with examples how each part of the form should be completed.

See **Template 1: 5x5x5 Information/Intelligence Report Form A.**

1.4.1 Government Protective Marking Scheme (GPMS)

The blank 5x5x5 form does not require any government protective marking and is headed **NOT PROTECTIVELY MARKED UNTIL COMPLETED,** see **Template 1.** Once the report contains information, however, it needs to be allocated an appropriate protective marking. There are five levels of this marking for sensitive assets, depending on the degree of sensitivity involved: **PROTECT, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET.** The majority of information/intelligence that the Police Service holds contains personal or sensitive data. This data, therefore, needs a level of protective marking and normally this will be **RESTRICTED.** The GPMS **TOP SECRET** marking is not included on the 5x5x5 as it is unlikely that this form would ever be used for such material.

Note: The **PROTECT** marking was introduced after the first edition of ***MoPI Guidance*** was published. It has not been added to the 5x5x5 given that it is unlikely to be used with sufficient frequency to justify the cost of changing the template on force systems.

For further information on the GPMS, see **Appendix 7** or contact the force Information Security Officer.

1.4.2 Reporting Member of Staff and Date/Time of Report

ORGANISATION AND OFFICER	*Sandford Police FIB* *PC 123 Smith*	DATE/TIME OF REPORT	*25/07/05* *10.08*

These fields record name, rank or position, station or office of the person who completes the Information/Intelligence Report, together with the date and time of submission.

1.4.3 Person Providing Information (Source)

INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE	*Mrs S Brown* *23 High Street Sandford or ISR /FIB/1234/05 (used to protect sensitive sources)*	REPORT URN	*12345/05*

The identification of the source of the information can either be the name and address of the person providing the information, or an intelligence source reference (ISR) number. Details of the person providing the information should be placed in these sections and not in the body of the text of the report. By providing this information on the 5x5x5, it allows for transparency in the possible identification of unauthorised CHIS and also for the continuation of the audit trail. For advice on ISR contact the local Dedicated Source Unit.

In many circumstances revealing the identity of the source on a 5x5x5 can result in compromising that source or a current operation. A 5x5x5 report derived from sensitive sources such as CHIS, covert or technical deployments and surveillance, should not reveal the true identity or nature of that source. In these circumstances a unique information/ intelligence source reference, referred to as an ISR, should be used.

A unique reference number (URN) will be added to the report by the receiving intelligence unit in order to provide an audit trail of received information.

Items of information from the same source but concerning totally different matters should be recorded on separate Information/ Intelligence Reports. A 5x5x5 report may, nevertheless, contain several items of information relevant to the same issue but they should all come from the same source. This is particularly important when intelligence reports are prepared from a sensitive source, for example, CHIS or a technical device. The purpose of this procedure is to ensure that an adverse decision on 'disclosure' of a 5x5x5 would only put a single sensitive source or a single record at risk of compromise.

For further information on the management of intelligence from CHIS and covert deployments, see ***ACPO and HMCE (2004) Manual of Standards for CHIS*** and ***ACPO and HMCE (2004) National Standards in Covert Investigations Manual of Standards for Surveillance.***

1.4.4 Source Evaluation

SOURCE EVALUATION	**A** Always Reliable	**B** Mostly Reliable	**C** Sometimes Reliable	**D** Unreliable	**E** Untested Source

Source reliability refers to the assessment given to the person, agency or technical equipment providing the information/ intelligence. The source reliability is assessed initially by the person recording the information and should be completed in all circumstances. Source evaluation is not a static process and should be subject to continual review. This will affect the whole of the information management process, particularly sharing information and the need for retaining it.

The assessment of the source should be based, as far as possible, on objective knowledge of the source as it will affect both the evaluation of the information recorded and any potential actions based on the information.

The 5x5x5 provides five gradings in respect of source evaluation.

A – ALWAYS RELIABLE

There is no doubt of the authenticity, trustworthiness and competence of the source. Information has been supplied in the past and has proved to be reliable in **all** instances. This grading should only apply to cases where reliability can be assured. This means that it will not be used frequently as a source evaluation. It is normally used only for information received from technical products, eg, DNA, interceptions, fingerprints and not usually for information gained from people, however unimpeachable, due to the possibility of human error. Even with technical products, its use should be carefully considered due to the risk of errors arising from interpretation.

Officers should remember that as this MoPI advice is a public document, then disclosure of a 5x5x5 with an A evaluation would carry a clear risk of a technical source being compromised.

B – MOSTLY RELIABLE

Information has been received from this source in the past and in the majority of instances has proved to be reliable. This could be the majority of law enforcement and other prosecuting agencies.

Example: Information received from police officers, some tested CHIS and agencies, eg, UKBA may be evaluated as this source evaluation.

C – SOMETIMES RELIABLE

Some of the information received from this source has proved to be both reliable and unreliable. Any information with this grading should generally not be acted upon without corroboration. Where a potential risk demands a response, the intelligence manager will need to obtain as much corroboration as possible before commissioning action.

Example: This grading may apply to CHIS or information received from the media or product of a technical deployment where the quality is poor.

D – UNRELIABLE

Information under this grading will refer to individuals who have provided information in the past which has routinely proved unreliable. There may be some doubt regarding the authenticity, trustworthiness, competency or motive of the source. Any information with this grading should not be acted on without corroboration.

Example: This grading could apply to information received from members of the public with a potentially malicious motive, eg, in neighbourhood disputes, or to information received from an individual with a history of making false allegations.

E – UNTESTED SOURCE

This grading refers to information received from a source that has not previously provided information to the person recording it. The information may not necessarily be unreliable but should be treated with caution. Corroboration of this information should be sought.

Example: This grading will usually apply to members of the public, and the majority of information received from Crimestoppers.

1.4.5 Information/Intelligence Evaluation

INFORMATION/ INTELLIGENCE EVALUATION	**1** Known to be true without reservation	**2** Known personally to the source but not to the person reporting	**3** Not known personally to the source but corroborated	**4** Cannot be judged	**5** Suspected to be false

It is essential than any information received or recorded should be evaluated for reliability. The evaluation will involve using objective professional judgement, and the value of the information must not be exaggerated to encourage that action be taken. The assessment of the reliability of the information will be based on the person recording it and their knowledge of the circumstances at that time.

The 5x5x5 provides five information/intelligence evaluation gradings.

1 KNOWN TO BE TRUE WITHOUT RESERVATION

This could be information generated from a technical deployment or an event which was witnessed by a law enforcement officer or prosecuting agency. Information received from technical deployments should be treated with caution as although the information may have been recorded accurately the content may be misinterpreted. This grading refers to first-hand information.

Example: An officer witnessed an incident or refers to live evidence.

2 THE INFORMATION IS KNOWN PERSONALLY BY THE SOURCE BUT NOT TO THE PERSON REPORTING

Information under this grading is believed to be true by the source although is not personally known to be so by the person recording the information. The information is provided second hand.

Example: A CHIS giving information which they know of first hand, to the person recording the information.

3 THE INFORMATION IS NOT KNOWN PERSONALLY TO THE SOURCE BUT CAN BE CORROBORATED BY OTHER INFORMATION

Information given may have been received by a source from a third party and its reliability has been corroborated by other information, eg, CCTV, other force systems.

Example: A CHIS has been told that Michael Brown has been seen driving a car, registration ABC 123. The PNC checks that Michael Brown is the registered keeper of car registration ABC 123.

4 THE INFORMATION CANNOT BE JUDGED

The reliability of this information cannot be judged or corroborated. Information with this grading should be treated with caution.

Example: Anonymous information received from members of the public that a crime has occurred but it is not possible to corroborate.

5 SUSPECTED TO BE FALSE

Information with this grading should be treated with extreme caution. This information should be corroborated by a reliable source before any action is taken. Any person applying this grade should justify within the body of the report why it is appropriate to use this grading.

Example: Malicious callers or a CHIS who is engaged in criminal activity and provides exaggerated information against others in order to deflect attention from themselves, or to prepare a defence of working for the police should they be arrested.

1.4.6 Information Content

REPORT				
NOMINAL: *Andrew Kent*	**DoB:** *21/12/79*	**NIB CRO:** *15643/99V* **(WHO)**		
OPERATION NAME/NUMBER (OPTIONAL):		**S**	**I**	**H**
Proposed robbery **(WHAT)** *Andrew Kent is planning an armed robbery at a bank in Sandford town centre* **(WHERE),** *exact location not known. This is to take place in 2 days time 27/07/05 when the next cash delivery is received.* **(WHEN)** *He will be using a red car, details unknown.* **(HOW)**		*B*	*2*	

This refers to the body of the text within the report. The information provided should be clear, concise and without abbreviations. The body of the report should contain all information, whether the person submitting believes it to be relevant or not. Where possible, the information should be corroborated and provenance established. This could be done, for example, through interrogation of other business areas, for example, Andrew Kent is confirmed on PNC as being the registered keeper of a red Ford Escort car registration number ABC 123.

The information content will commence with the full name of the subject nominal, if known, together with their date of birth and/or age and, where possible, any national identification number, eg, National Identification Bureau Criminal Records Office number.

For ongoing operations, the operational name or number may be added.

Having identified **who** the information relates to, the information should then clearly describe what is likely to occur, **where**, **when**, **why** and **how**, if known. If information is **not known**, then this should be clearly stated.

1.4.7 Submission of the 5x5x5

Once information has been recorded on a 5x5x5, the report should be submitted to the force/BCU intelligence unit by secure electronic or manual means. It will then be considered for its intelligence value based on research, source reliability, the content of the information and its actionable value against the force/BCU control strategy, intelligence requirement or other policing purpose.

1.4.8 Initial Use of the Handling Codes

Handling codes are designed to provide an initial risk assessment prior to recording material onto an intelligence system. They allow recording officers and others involved in the dissemination of intelligence material to easily record their decisions on the suitability or otherwise of sharing the intelligence with other parties.

The officer completing the 5x5x5 will not usually complete the handling code unless they are officers/staff involved in the intelligence discipline, for example, trained intelligence officers and specialists. Should the person first recording the information have concerns about disseminating the information, they should complete specific handling instructions and, in cases where the 5x5x5 handling codes are not considered to provide sufficient control options, a Risk Assessment Form C may be appropriate. The Form C should be attached to the 5x5x5 when it is submitted. Unless concerns are raised, the intelligence unit will review the Information/Intelligence Report and apply the appropriate handling code. It is, therefore, important that Form C contains a comprehensive evaluation of the risk; as without this, the intelligence unit may lack the information to make an appropriate determination of the handling code.

For further information on the application of handling codes, see **1.5.5 Handling Codes of Appendix 2.**

1.4.9 Responsibilities

All staff should be able to identify information which may be relevant to policing purposes. They should also be able to complete an Information/Intelligence Report and identify obvious risks about the information.

The person submitting the 5x5x5 should check the information they wish to record against other business areas before entry, to help verify the information. Anyone submitting information has a duty to ensure that it is as accurate as possible and, where it can be easily corroborated, that action is taken. The first stage of converting what may be rumour into information that can be used, is for the reporting officer to ensure that the facts are accurate.

Checklist 5

Recording Information on a 5x5x5

The person completing a 5x5x5 must:

- Complete all submission fields.
- Assess the source reporting the information and apply the correct grading.
- Evaluate and grade the information given.
- Complete the text of the report.
- Use the correct GPMS marker.
- If necessary, give specific handling instructions and apply a risk assessment to the information. Where that is done, the Risk Assessment Form C should be attached and sent to the intelligence unit.
- Send the report to the appropriate intelligence unit in line with force security policy.

1.5 Evaluation of the 5x5x5

Once a 5x5x5 has been received by the intelligence unit, it will be further assessed for:

- Compliance with this guidance for the completion of 5x5x5 reports;
- Risks and duty of care issues, including CHIS safety;
- Its intelligence value;
- Consideration for further research and development;
- Consideration for dissemination and requirements for sanitisation;
- Entry onto the intelligence system.

1.5.1 Quality Assurance of the 5x5x5

When the 5x5x5 has been received, the initial report should be quality assured. The information contained within the 5x5x5 should be checked for completeness and accuracy.

Appropriate use of information is a key competency for all staff and is integral to the management of performance at personal and team levels.

Any amendment to the 5x5x5 should have an audit trail. This may include the resubmission of a sanitised 5x5x5, with an explanation for the amendment and details of the person making it.

1.5.2 Re-Evaluation of the Source and Information

The content of the 5x5x5 should be read and reviewed by the nominated intelligence officer with responsibility for quality assurance within the intelligence unit. The 5x5x5 will be examined in line with the initial gradings given. Reliance should be placed on the person submitting the report with regards to the source reliability and information evaluation unless there is an obvious discrepancy or incompatibility. If further clarity or corroboration is required on any issue, contact should be made with the person who submitted the report.

1.5.3 GPMS

The intelligence unit should note the GPMS (Government Protective Marking Scheme) marking contained on the 5x5x5. When quality assuring the 5x5x5, the document's protective marking should be checked to make sure it has the correct one attached to it, see **Appendix 7.**

1.5.4 Sanitisation

Reports should be sanitised for onward transmissions by removing material which explicitly or implicitly identifies a sensitive source. The text (as opposed to the source reference) should give no indication of the nature of the source. Persons should not put material into a 5x5x5 that adds no value or leads to the identification of the source or any sensitive operational details. For example, care should be taken not to reveal sensitive police tactics such as observation points, surveillance, covert human intelligence sources or other confidential information.

If the intelligence unit needs to sanitise the 5x5x5 before dissemination or inputting onto an intelligence system, a new 5x5x5 should be submitted. The new report should be given a new unique reference number (URN) and also be cross-referenced to the original report to identify provenance and provide an audit trail. The original report should be retained but stored securely to ensure that the source is not revealed.

The following examples highlight specific issues, and then illustrate good practice for recording information.

Example 1:

5x5x5 report – Yesterday I met the informant John Clarke at 12.00 hrs at the dog track. He said the day before he was round at Tommy Smith's place and he overheard him on the phone. Tommy said there wouldn't be a problem, he'd got enough cash and he would take as much speed and coke as the man could provide him with, but that he didn't want any smack this time.

The informant said he did 1471 on the phone and the number that came back was 01123 456789.

Problem – The Information/Intelligence Report places the source at a known location at a known time and could lead to their identification. It also highlights that the source is human.

Best practice – Intelligence suggests that Thomas Smith is involved in the purchase and supply of controlled drugs. Intelligence suggests that the telephone number 01123 456789 has been in contact with Tommy SMITH.

Example 2:

5x5x5 report – At approximately 10.00 hrs on Saturday 27th February, 1999 the subject Richard Smith was seen from an observation post at number 2 High Street, Anytown to return home driving a red Saab A123 ABC.

Problem – The report identifies the source of the information, the identity of the person assisting the police and the location of the observation post.

Best practice – Richard SMITH is currently using a red Saab registration number A123 ABC. (PNC information or details of SMITH's home address would be attached to the Officer Notes/Intelligence Unit Notes/Action field of the sanitised 5x5x5 form and NOT in the body of the text.)

Or

Richard SMITH was in the High Street, Anytown at 10:00 on 27 February 1999 using a red Saab A123 ABC

(This log would be considered for restricting on a force's intelligence system if the High Street in question was very quiet and there was only a small chance of a person seeing SMITH.)

Example 3:

5x5x5 report – From a camera installed at premises looking onto 1 High Street, Anytown, John Doe called on Fred Smith at 11:00 hrs on Tuesday 12 January and Smith passed a package to Doe.

Problem – This reveals a technical source and could reveal its location.

Best practice – Intelligence indicates that John Doe collected a package from Fred Smith on Tuesday 12 January. Depending on the nature of the operation this could be further broken down into three logs:

1. John DOE and Fred SMITH are associates.
2. On Tuesday 12 January, Fred SMITH passed a package to John Doe.
3. John DOE and Fred SMITH were together at 1 High Street on 12 January.

For further guidance on sanitisation, see ***ACPO and HMCE (2004) Manual of Standards for Covert Human Intelligence Sources.***

1.5.5 Handling Codes

HANDLING CODE To be completed by the evaluator on receipt and prior to entry onto the intelligence system. **To be reviewed on dissemination.**	**1** **Default:** Permits dissemination within the UK Police Service **and** to other law enforcement agencies as specified. [See guidance] ☐	**2** Permits dissemination to UK non-prosecuting parties. [Conditions apply, see guidance] ☐	**3** Permits dissemination to (non EU) foreign law enforcement agencies. [Conditions apply, see guidance] ☐	**4** Permits dissemination within originating force/agency only: specify reasons and internal receipient(s) Review period must be set. [See guidance] ☐	**5** Permits dissemination but receiving agency to observe conditions as specified. [See guidance on risk assessment] ☐

Handling codes are designed to assist the intelligence unit in the risk assessment decision of whether to disseminate intelligence or not and, if so, to whom. The codes provide clarity over the purpose for communicating the piece of intelligence to others. By recording this on the 5x5x5, it clearly outlines the conditions which should be met when disseminating that specific piece of intelligence to other parties. Only persons trained in applying handling codes, for example, those in the intelligence unit should apply them. The person should have an overview of other information which is relevant in the dissemination of the intelligence.

Individual officers and designated employees of the police are authorising officers for the purpose of disseminating intelligence material to other law enforcement and prosecuting agencies.

Before a decision to disseminate is made, the intelligence unit should apply one of the five handling codes. All the handling codes allow dissemination of the information where appropriate.

CODE 1 – DEFAULT: PERMITS DISSEMINATION WITHIN THE UK POLICE SERVICE AND TO OTHER LAW ENFORCEMENT AGENCIES AS SPECIFIED

This handling code permits intelligence to be disseminated within the UK Police Service and other law enforcement agencies, which must be specified. Under this code the Police Service is defined in its entirety and not just a local force area.

This is the **default** code for general dissemination to the Police Service and will directly link to the development of common person records across the organisation.

The use of this code permits dissemination to a wide range of police and law enforcement agencies, but only those agencies with a specific need to know the information will receive it.

For the purpose of this handling code, other law enforcement agencies include SOCA, the United Kingdom Border Agency and Europol. Prosecuting agencies are regarded as law enforcement agencies for the purpose of this handling code including the Crown Prosecution Service, the Department of Work and Pensions and local authority departments, for example, Trading Standards.

Example: Information that Andrew Brown, a convicted drug dealer, is currently using a red Ford Escort ABC 123 to transport Class A drugs between London and Birmingham. No current ongoing operation exists in relation to Brown in the reporting force, Handling Code 1 applies to disseminate across the Police Service.

Information that Bob Clark, who has a fleet of lorries travelling Europe and the UK, is believed to be involved in people smuggling, dropping off illegal immigrants at motorway service areas. Handling Code 1 applies as the information would need to be disseminated to the whole Police Service and United Kingdom Border Agency.

CODE 2 – PERMITS DISSEMINATION TO UK NON-PROSECUTING PARTIES

This handling code permits intelligence to be disseminated to non-prosecuting parties in the UK. For the purpose of this handling code, non-prosecuting parties include commercial organisations such as credit card companies.

This code can permit the dissemination of certain relevant information but will not necessarily require the full record to be disclosed.

When intelligence is disseminated to non-prosecuting parties, a record should be kept of the recipient, the material disseminated, the purpose of dissemination, the authorisation and any restrictions on the use or further dissemination of the information. In some cases Form C may be appropriate. Any intelligence which is disseminated to non-prosecuting parties should be authorised by an officer of at least inspector or equivalent.

Example: Information received that Jane Smith is planning to open a number of mail order catalogue accounts in a false name as she is registered bankrupt. Handling Code 2 applies, the information is appropriate for dissemination to the applicable commercial organisation as this likely offence can best be tackled by passing the information on to the partner who is able to intervene immediately and prevent it.

CODE 3 – PERMITS DISSEMINATION TO (NON-EU) FOREIGN LAW ENFORCEMENT AGENCIES

This handling code permits intelligence to be disseminated to non-EU foreign law enforcement agencies. In the case of non-EU law enforcement agencies, forces should risk assess each on an individual basis.

This code arises directly from the requirement of the Data Protection Act for personal information to be disseminated outside the EU only after the risks have been assessed and on the grounds of substantial public interest. Public interest in this context will include tackling serious crime and the maintenance of the security and integrity of law enforcement agencies.

Dissemination outside the UK is managed by SOCA.

Example: Information is received that a dangerous paedophile currently living in the UK is moving abroad to Thailand. Handling Code 3 applies as the intelligence could be sent to the authorities in Thailand.

CODE 4 – PERMITS DISSEMINATION WITHIN ORIGINATING FORCE/AGENCY ONLY – SPECIFY REASONS AND INTERNAL RECIPIENT(S)

This handling code restricts the dissemination of the intelligence to the originating force/agency. It provides for the need to retain particularly sensitive information within a tight community with a specific need to know. It is likely to be of use in restricting access to material that is relevant to current sensitive operations. This may include restricting dissemination to a particular operational team within that force or agency.

Prior to applying this handling code, a rigorous evaluation should take place to justify why further dissemination is not appropriate. Any intelligence report given a Code 4 **should** remain under constant review to ensure that wider dissemination can occur as soon as is feasible, such as when an operation has been concluded or is no longer being pursued.

There will be an assumption that any information/intelligence marked with this grading will not be further disseminated without contacting the originator of the report.

This is not the default handling code.

Example: Information received from an undercover officer currently deployed in a long-term class A drugs infiltration operation states that one of the operational targets has had meetings in another force area. This reveals the identity and current activity of suppliers in that force area. The undercover officer is currently the only other person who can possibly know of those contacts. Handling Code 4 applies as dissemination outside of the undercover operational team is likely to seriously compromise the officer and operation. In this situation a risk assessment Form C may be used. An authorising officer should stipulate regular review. Handling Code 4 does not prevent the release of some of the relevant material where sanitisation is possible although the whole report cannot be disseminated at this point.

CODE 5 – PERMITS DISSEMINATION BUT RECEIVING AGENCY TO OBSERVE CONDITIONS AS SPECIFIED

Any information marked with this handling code requires special attention. Application of this code means the originator has applied specific handling instructions in respect of this information. It is possible that a Risk Assessment Form C will be required in respect of the information concerned and that if it is subsequently used in court, an application for Public Interest Immunity will be sought. Where handling code options are insufficient against the perceived risk of the information to a source, a Form C should be completed.

Example: Information from a CHIS relating to potential serious harm to a child is deemed suitable for dissemination to social services. Due to the sensitive nature of the information, the social services department receiving it may only use this information in a confidential case conference rather than at an open forum. Handling Code 5 applies, subject to the completion of a further risk assessment Form C.

1.6 Form C – Additional Risk Assessment

Form C is a method by which information/intelligence received through the 5x5x5 process can be risk assessed, see **Template 3.**

If there are concerns regarding the source of the information or where a risk to others is identified, a Form C must be completed and included with the report.

A further risk assessment will take place when the report is evaluated for dissemination and the handling codes are applied. It may be appropriate for the person evaluating the report and applying a handling code to use a Form C at any time.

The risk assessment process also includes consideration of ethical, personal and operational risks in respect of the source, the information content, its use, dissemination and compliance with a legislative requirement or policing purpose.

This process will also include a justification for the decisions made and the appropriate authority of the person making them. It will consider the proportionality, accountability and necessity for recording, disseminating and retaining the information.

Ethical risks

Assessments of ethical risks concern the issues of proportionality and necessity (justification), including addressing the following questions:

- Is the recording or dissemination of the intelligence proportionate to the problem it is intended to solve?
- Does the recording or dissemination of the intelligence comply with the policing purposes?
- Does the intelligence contain material relating to persons other than the target? Are the risks of such collateral intrusion being passed on acceptable? Can the risk be sifted out?
- Does the character and standing of any individual concerned have any impact on proportionality? An individual's character needs to be taken into account when considering the issue of proportionality. If someone has a string of convictions for similar offences, proportionality of any proposed action may become less of an issue than if the person was of previous good character.

Personal risks

Assessment of the personal risks includes addressing the following questions:

- Is there a risk of personal injury to the target, the public or a member of the law enforcement agencies?
- Are there any obvious physical risks faced by operatives involved in any operation reliant on the use of the material? (Where the intelligence leads to an operational response, for example, a covert operation, the techniques employed will also be risk assessed.)

- Are there risks to the safety of the target, or individuals who may assist the law enforcement agencies or be subject to collateral intrusion, for example, the source?
- Are the risks to the data subject, arising from the dissemination of the intelligence material, acceptable?

Operational risks

Assessment of operational risks includes addressing the following questions:

- Is there a risk of disproportionate damage to the professional reputation of the force should the intelligence be exposed or a prosecution collapse?
- Is there a risk of damage to community relations in the event of a compromise?
- Would exposure by disclosure or any other event compromise a sensitive technique, a current operation or a source?
- Does the intelligence contain confidential material? If so, before the material can be recorded onto an intelligence system or disseminated, due account should be taken of any restrictions on its use or requirement for special handling imposed by the officer who authorised its collection. An assessment should be made of the risks arising from the use of the material, or from its potential disclosure in court proceedings. The Risk Assessment process must be carried out on Form C, see **Template 3.**

1.7 Responsibilities

The Intelligence Unit should ensure that all intelligence is managed in line with this guidance. Once a person has submitted a 5x5x5 for the Intelligence Unit's attention, there is an expectation that the intelligence will be properly evaluated and considered for appropriate dissemination.

For roles and responsibilities of Information and Intelligence Management, see ***ACPO (2005) Guidance on the National Intelligence Model*, Section 4 People Assets.**

Checklist 6

Evaluation of the 5x5x5

On receipt of a 5x5x5, the following actions should be taken:

- Quality assure the original 5x5x5 for its completeness and accuracy;
- Re-evaluate the reliability of the source and information;
- Apply the GPMS marking;
- Sanitise the content if appropriate;
- Apply the appropriate handling code;
- Complete a Risk Assessment Form C, if needed.

1.8 Intelligence Actioning Process

Once information within the 5x5x5 has been reviewed, the appropriate handling codes applied and the required level of authorisation obtained, it may be actioned and entered into the intelligence system. A priority assessment process for the information may be adopted at this stage to manage workload and resources, while ensuring that the highest priority intelligence is actioned at the earliest opportunity.

1.8.1 Priority Assessments

A priority assessment can determine the appropriate action for a specific piece of information.

The priority assessment may change over time depending on research and development. The application of this process will usually take place in the Intelligence Unit because of the nature of the information recorded, evaluated and held in the intelligence business area.

Priority assessments are dynamic and affected by a number of factors. The protection of particular members of society such as children and vulnerable adults will always have a bearing on priority assessments, see **2.3 Critical Information Areas.** Other priority assessments will be agreed locally at force or BCU level and will depend on the control strategy and the policing priorities for the area in question.

The following priority assessment criteria are intended as a guide, but will be set at a local force level.

Priority Assessment HIGH (H): Risk of Serious Harm

- This refers to information which indicates a risk of death and/or serious harm.
- The information could relate to the imminent commission of other serious crime.
- When a piece of information is assessed as high priority, it should be marked as such and immediately brought to the attention of the appropriate supervisor and actioned. This action should include further evaluation and risk assessment against known or believed facts and its immediate entry onto the intelligence system should be considered

Example: A reliable source states Michael Brown, a known offender, has a shotgun (confirmed on firearms licensing register) and intends to shoot Simon Smith. The name of the victim is known, the name of the offender is known and there is, potentially, a public and officer safety issue here.

Priority Assessment MEDIUM (M): NIM Control Strategy/ Intelligence Requirements/Current Operation/High-Risk Issue

- This refers to information focused on NIM Control Strategy Areas, intelligence requirements, any current operations or information relating to a high-risk offender or an offence that may not be committed imminently, such as a sex/dangerous/violent offender who has been released on licence.
- There is an expectation that information assessed as a medium priority will remain subject to further evaluation, risk assessment and development, and consideration for early entry onto the intelligence system.

Example: A reliable source states Simon Smith and Michael Brown intend to commit a dwelling house burglary on the High Street some time this week. Burglary is part of the BCU control strategy and intelligence requirement. The High Street is subject to a current problem profile in respect of dwelling house burglaries.

Priority Assessment LOW (L): Other Information

- This is information which falls outside the parameters of high and medium priorities. The information has been recorded as it meets the policing purpose criteria, and could also relate to matters that would benefit from further research and development. Such information may identify emerging trends and issues or problem localities which will inform the NIM process, see ***ACPO (2005) Guidance on the National Intelligence Model.***

- This information requires evaluation and risk assessment and needs to be recorded appropriately.

Example: A reliable source states that Michael Brown and Simon Smith intend to go shoplifting in the town centre. They do this on a regular basis. Shoplifting is not part of the BCU control strategy or intelligence requirement. The information is relevant for the purposes of the prevention and detection of crime, and is recorded accordingly. Further research and development may assist in developing target profiles and intervention strategies against Brown and Smith who, as well as shoplifting, are known to be active in a number of other types of crimes.

1.8.2 Authorisations

5x5x5 REVIEWED BY: RE-EVALUATED: Yes ☐ No ☐	CROSS-REF URN:	TIME/DATE OF REVIEW:
DISSEMINATED TO:	PERSON DISSEMINATING TIME/DATE:	
DETAILED HANDLING INSTRUCTIONS:	PUBLIC INTEREST IMMUNITY:	
INPUT ONTO AN INTELLIGENCE SYSTEM Yes ☐ No ☐		
SIGNATURE (PAPER COPY):		

Individual officers and designated employees of the police, including the Scottish DEA and SOCA, are self-authorising officers for the purpose of their duty to record intelligence material.

Individual officers are responsible for making the decision to record information on a 5x5x5. Before recording intelligence material, the officer should be satisfied that:

- The activity conforms to a policing purpose;
- The intelligence to be recorded onto intelligence systems has been properly evaluated and its provenance established;
- Where the intelligence is to be recorded onto intelligence systems for later action, it has been assessed for risks arising from its use or from its potential disclosure in court proceedings;
- Any linked 5x5x5 reports are cross-referred by a URN;
- Any changes to the original 5x5x5 should have been audited by the Intelligence Unit;
- Any paper copy 5x5x5 has been signed by the authorising officer.

1.8.3 Entry onto an Intelligence System

NIM identifies a number of key roles and functions responsible for information IT management and data entry. NIM also provides details of minimum standards which specify that there should be sufficient resources available to carry out data entry and to ensure that its quality is maintained. For further information see ***ACPO (2005) Guidance on the National Intelligence Model,*** **Section 4 People Assets** and **Appendix 2.**

Once authority has been given for data to be entered onto the intelligence system, persons responsible for its input should have regard to the appropriate handling code, specific handling and dissemination instructions, and any risk assessments. This will ensure that all data entry complies with the instructions of the authorising officer.

For guidance on subsequent review and retention of any intelligence material recorded, see **7 Review, Retention and Disposal.**

Template 1

NOT PROTECTIVELY MARKED UNTIL COMPLETED

GPMS:	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

5x5x5 Information Intelligence Report Form A

ORGANISATION AND OFFICER		DATE/TIME OF REPORT	
INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)		REPORT URN	

SOURCE AND INFORMATION/INTELLIGENCE EVALUATION TO BE COMPLETED BY SUBMITTING OFFICER

SOURCE EVALUATION	**A** Always Reliable	**B** Mostly Reliable	**C** Sometimes Reliable	**D** Unreliable	**E** Untested Source
INFORMATION/ INTELLIGENCE EVALUATION	**1** Known to be true without reservation	**2** Known personally to the source but not to the person reporting	**3** Not known personally to the source but corroborated	**4** Cannot be judged	**5** Suspected to be false

REPORT

PERSON RECORD:	**DoB:**	**NIB CRO:**

OPERATION NAME/NUMBER:	**S**	**I**	**H**

INTELLIGENCE UNIT ONLY

HANDLING CODE	**1**	**2**	**3**	**4**	**5**
To be completed by the evaluator on receipt and prior to entry onto the intelligence system. **To be reviewed on dissemination.**	**Default:** Permits dissemination within the UK Police Service **and** to other law enforcement agencies as specified. [See guidance] ☐	Permits dissemination to UK non-prosecuting parties. [Conditions apply, see guidance] ☐	Permits dissemination to (non EU) foreign law enforcement agencies. [Conditions apply, see guidance] ☐	Permits dissemination within originating force/agency only: specify reasons and internal recipient(s) Review period must be set. [See guidance] ☐	Permits dissemination but receiving agency to observe conditions as specified. [See guidance on risk assessment] ☐

5x5x5 REVIEWED BY: RE-EVALUATED: Yes ☐ No ☐	CROSS-REF URN:	TIME/DATE OF REVIEW:
DISSEMINATED TO:	PERSON DISSEMINATING TIME/DATE:	
DETAILED HANDLING INSTRUCTIONS:	PUBLIC INTEREST IMMUNITY:	
INPUT ONTO AN INTELLIGENCE SYSTEM Yes ☐ No ☐		
SIGNATURE (PAPER COPY):		

GPMS:	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

Template 2

NOT PROTECTIVELY MARKED UNTIL COMPLETED

GPMS:	RESTRICTED ☐	CONFIDENTIAL ☐	SECRET ☐

5x5x5 Continuation Form B

INFORMATION/INTELLIGENCE SOURCE/INTELLIGENCE SOURCE REF NO. (ISR)		REPORT URN	
REPORT			
NOMINAL:	DoB:	NIB CRO:	
OPERATION NAME/NUMBER:			**S** **I** **H**
GPMS:	**RESTRICTED** ☐	**CONFIDENTIAL** ☐	**SECRET** ☐

Template 3

Risk Assessment Form C

FOR THE USE IN DISSEMINATION OF INFORMATION/INTELLIGENCE

1	Does the information contain confidential material or sensitive material as identified in law?	**YES/NO**
2	If yes, are there any restrictions on use, or requirements for special handling, imposed by the person submitting the report?	**YES/NO**
3	What are the ethical, personal or operational risks which are likely to result as a consequence of any dissemination or disclosure? Consideration must be given to the risk to the source and the content of information within the report.	**DETAIL THE RISKS**
4	What is the purpose of dissemination or disclosure? Is it for a policing purpose or a legislative requirement?	
5	Having identified the risks, justify the decision-making process. This must include the justification, authority, proportionality, accountability and necessity of a dissemination or disclosure.	
FOR INTELLIGENCE UNIT ONLY		
6	In light of the risk assessment is the Handling Code correct?	**YES/NO**
Risk Assessment and Management Plan authorised by ..... (Intelligence Manager)		**Person Completing Risk Assessment:**
Cross-ref URN:		**Time/Date:**

Appendix 3

Information Sharing Agreement

INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

SANDFORD DISTRICT COUNCIL

AND

WESTSHIRE CONSTABULARY

Version 1.0

Contents

SUMMARY SHEET

Title of ISA

ISA Ref:	WC001/SandfordDC

PURPOSE	To take action against crime and anti-social behaviour in properties owned and managed by Sandford District Council.

PARTNERS	Westshire Constabulary Sandford District Council

Date Agreement comes into force:	01/01/06

Date Agreement Review:	01/07/06

Agreement Owner:	Westshire Constabulary

Agreement drawn up by:	Inspector Bob Jones

Location of Agreement in force:	S:Information Sharing/Housing/Sandford

Protective Marking:	Not Restricted

VERSION RECORD

Version No.	Amendments Made	Authorisation
001	First Version	Chief Supt Evans

1 Introduction

1.1 Westshire Constabulary is committed to partnership working and is continually looking for opportunities to work more closely with local authorities and other social housing landlords to detect, prevent and reduce crime and anti-social behaviour.

1.2 This agreement outlines the need for the police and housing providers to work together to alleviate crime and anti-social behaviour in social housing areas, and provides a framework for action.

2 Purpose

2.1 This purpose of this agreement is to enable action to be taken against crime and anti-social behaviour in properties owned and managed by Sandford District Council. It will incorporate measures aimed at:

- Facilitating a coordinated approach that targets crime and anti-social behaviour;
- Facilitating the collection and exchange of relevant information;
- The pursuit of civil or criminal proceedings – either by Westshire Constabulary or Sandford District Council;
- Ensuring that the sharing of information meets one or more of the policing purposes.

2.2 It also seeks to increase the confidence of residents, while encouraging their support, to enable Westshire Constabulary and Sandford District Council to combat crime and anti-social behaviour.

3 Partners

3.1 This agreement is between the following partners:

SANDFORD DISTRICT COUNCIL of 2–5 Ford Lane, Sandford, Westshire

WESTSHIRE CONSTABULARY of County House, Westshire.

4 Power(s)

4.1 This agreement fulfils the requirements of the following:

- Housing Act 1985 and 1988 (schedule 2, grounds 2 and 14);
- Housing Act 1996 (sections 135, 152 and 153);
- The Protection from Harassment Act 1997;

- The Homelessness Act 2002;
- The Civil Evidence Act 1995;
- The Crime and Disorder Act 1998 (section 115);
- Common Law Powers of Disclosure;
- The Rehabilitation of Offenders Act 1974;
- The Human Rights Act 1998 (Article 8);
- The Data Protection Act 1998 (sections 29(3) and 35(2).

5 Process

5.1 This agreement has been formulated to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared should be justified on the merits of each case.

5.2 TYPES OF INFORMATION TO BE SHARED

Westshire Constabulary will share:

- Depersonalised information relating to crime or anti-social behaviour in the areas of housing owned or managed by Sandford;
- Evidence relating to a conviction of a tenant for a criminal offence which occurred in the property or in the vicinity of the property, providing that the offence is not considered spent under the Rehabilitation of Offenders Act 1974;
- Evidence relating to a caution accepted by the tenant for a criminal offence that occurred in the property or in the vicinity of the property owned by Sandford District Council, where the date of the caution is less than twelve months from the disclosure date;
- Evidence of warnings given under the Harassment Act 1997, where warnings are recorded by the police against the tenant or invited visitor to, or in the vicinity of, the property within a period of twelve months;
- An admission of anti-social behaviour by the tenant, member of the resident family or invited visitor, evidenced by a pocket notebook signature by the offender;
- Evidence from police records of incidents of anti-social behaviour at, or in the immediate vicinity of, the tenant's accommodation where there is evidence that these were committed by the tenants, their resident family or invited visitors;
- Copies of statements made to the police by third parties where written permission has been provided by the person making the statement for it to be disclosed for use in civil proceedings.

Sandford District Council will share:

- Evidence, including complaints from neighbours or the public relating to criminal or anti-social behaviour at, or in the immediate vicinity of, the tenant's accommodation where there is evidence that these were committed by the tenants, their resident family or invited visitors.

5.3 CONSTRAINTS ON THE USE OF THE INFORMATION

5.3.1 The information shared should not be disclosed to any third party without the written consent of the agency that provided the information. It should be stored securely and deleted when it is no longer required for the purpose for which it is provided.

5.4 ROLES AND RESPONSIBILITIES UNDER THIS AGREEMENT

5.4.1 Each partner should appoint a single point of contact (SPoC) who should work together to jointly solve problems relating to social tenants. The sharing of information should only take place where it is valid and legally justified.

5.4.2 SPoCs should meet regularly to discuss and prioritise incidents of criminal or anti-social behaviour. Both contacts have a responsibility to create a file or folder that can record each individual request for information and the decision made. It should include copies of the request for information, details of the data accessed and notes of any meeting, correspondence or phone calls relating to the request.

5.4.3 Any request for information should meet one or more of the policing purposes.

5.4.4 Within Westshire Constabulary, the file should be held and managed centrally by a Force Information Manager. This arrangement should be replicated within Sandford District Council.

5.4.5 The designated police officer should ensure that the request meets a policing purpose. Where the information refers to a victim or witness, their written consent must be obtained.

5.5 SPECIFIC PROCEDURES

5.5.1 Handling Requests for Information – all requests for information must be made in writing using the 'Request for Personal Information' form.

5.5.2 Requests may be made by fax but care should be taken where personal information is shared. Similarly, requests and replies should not be communicated via email as the internet is not secure for the transition of personal and sensitive personal information.

5.5.3 Requests for information may be made by telephone in cases of emergency, for example, where there is a risk of immediate violence. Where this occurs, the request for information must be recorded on Form A and submitted retrospectively.

5.5.4 Replies to requests must be made within ten working days.

5.5.5 Information Requested by Sandford DC Prior to Conviction or Caution:

5.5.6 In some cases it may be more appropriate to take civil action rather than prosecute. Where this occurs, it will be the responsibility of the police to determine whether or not they will support civil proceedings.

5.5.7 Where the local authority requests information about a particular individual after a criminal investigation has already started, any decision on whether or not to proceed with a criminal prosecution should be referred to the designated police officer, who will liaise with the Crown Prosecution Service. This is particularly important in cases involving child abuse, domestic violence and incidents where Covert Human Intelligence Sources (CHIS) have been tasked.

5.5.8 Where a criminal prosecution is pending and the local authority wishes to pursue civil proceedings in advance of a prosecution, a police officer can only provide factual information with the prior consent of the Crown Prosecution Service. The police cannot provide opinion evidence.

5.5.9 Where a complaint of anti-social behaviour has been made against a tenant, both partners can share information (providing that it meets a policing purpose and satisfies the principles of the Data Protection Act) to help decide what course of action, if any, to take against the tenant. Such disclosures will only deal with the incident or offences that have occurred in the premises or in the immediate vicinity, and will be aimed at deciding on the course of joint action, if required. All decisions must be recorded.

5.5.10 Where more serious allegations are made against the tenant, the nominated officer from Sandford DC must write to Westshire Constabulary informing them that action is being considered. The tenant's name and address should be shared with the police to enable officers to carry out a search. This may include details on:

- Events witnessed by a police officer;
- Evidenced incidents at the address or the immediate locality;
- Warrants executed;
- Persons arrested.

5.5.11 Officers attending incidents should make detailed pocket book entries of any complaints or statements obtained during criminal investigations. These complaints or statements can only be shared with the local authority with the individual's written permission and only once the criminal proceedings have been completed.

5.5.12 Information Requested by the Local Authority Post Conviction or Caution:

5.5.13 Where the criminal process is complete, copies of relevant police statements may be released to the local authority. Statements obtained from witnesses will also be released provided the appropriate written consent has been given.

5.5.14 Care must be taken not to disclose convictions that are spent within the meaning of the Rehabilitation of Offenders Act.

5.6 REVIEW, RETENTION AND DISPOSAL

5.6.1 Partners to this agreement undertake that personal data shared will only be used for the specific purpose for which it is requested. The recipient of the information is required to keep it securely stored and will dispose of it when it is no longer required. The force may also wish to request a copy of the partner's information security policy (where it exists) when sensitive personal data is to be shared.

5.6.2 Files containing information from partner sources will be reviewed in line with force policy.

5.6.3 The recipient will not release the information to any third party without obtaining the express written authority of the partner who provided the information.

5.7 REVIEW OF THE INFORMATION SHARING AGREEMENT

5.7.1 The ISA will be reviewed six months after its implementation and annually thereafter. The nominated holder of this agreement is Westshire Constabulary. It is based on the national template for Information Sharing, which forms part of ***ACPO (2010) Guidance on the Management of Police Information,*** **Second Edition.**

5.8 INDEMNITY

5.8.1 Sandford District Council as receivers of police information will accept total liability for a breach of this Information Sharing Agreement should legal proceedings be served in relation to the breach.

6 Signature

6.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself are sufficient to meet the purpose of this agreement.

6.2 Signatories must also ensure that they comply with all relevant legislation.

Signed on behalf of Westshire Constabulary:

.....

Title: .....

Rank/Position: .....

Date: .....

Signed on behalf of Sandford District Council:

.....

Title: .....

Rank/Position: .....

Date: .....

RESTRICTED (when complete)

Request for Personal Information Form

i am requesting personal information or sensitive personal information under the Data Protection Act 1998 about:

Our Ref:	
Surname:	
All previous surnames:	
Also known as:	
Forenames:	

Place of Birth:		Date of Birth:	

Full Present Address:	
Postcode:	
Previous Address:	
Postcode:	

The information i require is:

i confirm that the personal or sensitive personal information is required for the following purpose:

Failure to provide the information will result in:

Signed		Date	
Name		Rank/Title	

RESTRICTED (when complete)

Appendix 4

National Retention Assessment Criteria

Review Schedule

Contents

APPENDIX 4(i) – National Retention Assessment Criteria

For advice on completion of this form, see **7.4 National Retention Assessment Criteria** of this guidance.

Record:	
Date of Review:	
Review Type (Triggered or Scheduled):	

If review was triggered explain how/why:

Retention Criteria

Factors – Risk of Harm	Yes/No	If 'Yes' provide an explanation of how/why:
1. Is there evidence of a capacity to inflict serious harm, eg, threats, violence towards partner, hate-based behaviour, predatory behaviour?		
2. Are there any concerns in relation to children or vulnerable adults?		
3. Did the behaviour involve a breach of trust?		
4. Is there evidence of established links or associations which might increase the risk of harm, eg, gang membership, contact with known paedophiles or other established criminal groups?		
5. Is there evidence of substance misuse?		
6. Are there concerns about the individual's mental state, eg, symptoms of mental illness, obsessive or compulsive behaviour, morbid jealousy, paranoia, lack of self-control?		
7. Any other reasons?		

Is the information under review proportionate and still necessary for a policing purpose?	**Yes/No**
Is the information under review adequate and up to date?	**Yes/No**

Outcome of Review:

Completed by:

Authorised by:

APPENDIX 4(ii) – Review Schedule

Review Group	Offence/Record Type	Action	Rationale
Group 1			
Certain public protection matters.	1. MAPPA managed offenders. 2. Serious offence specified in CJA 2003. 3. Potentially dangerous people.	Retain until subject has reached 100 years of age. Review every 10 years to ensure adequacy and necessity.	This category poses the highest possible risk of harm to the public.
Group 2			
Other sexual and violent offences.	Sexual offences listed in Schedule 3 Sexual Offences Act 2003. Violent offences specified in the Home Office counting rules for recorded crime/National Crime Recording Standard. 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 such on the PNLD.	Review after an initial 10 year clear period. If subject is deemed to pose a high risk of harm retain and review after a further 10 year clear period.	National Retention Assessment Criteria – Appendix 4(i).
Group 3			
All other offences.	All other offences.	Retain for initial 6-year clear period. Either review and risk assess every 5 years or carry out time-based disposal depending on force policy.	Lower risk of harm. Forces must balance the risk posed by this group with the burden of reviewing.

APPENDIX 4(ii) – Review Schedule continued

Review Group	Offence/Record Type	Action	Rationale
Group 4			
Undetected crime.	Serious specified offences. Other offences.	Retain records for 100 years from the date the crime was reported to police. A minimum of 6 years.	CJA 2003. Limitation Act 1980.
CRB disclosures.	Information disclosed under Part 5 of the Police Act 1997.	Retain for 10 years from date of request.	CRB Quality Assurance Framework.
Intelligence products.	Target Profiles. Association Diagrams.	Review according to crime type as outlined in categories 1-3.	
Missing persons.	Resolved. Unresolved.	Retain for a minimum of 6 years. Dispose of if this period has been 'clear' and there are no further indicators of risk. Retain until resolved.	Limitation Act 1980.
Victim/witness details.		Retain for a minimum of 6 years or length of sentence if this is longer. Decisions to dispose of must be made on a case-by-case basis. Retain if victim/witness is recorded as the offender/suspect for another offence.	Limitation Act 1980. CPIA 1996.

Appendix 5

Glossary

This appendix covers the main terms, abbreviations and acronyms used within the guidance.

Glossary

Basic Command Unit (BCU)
A geographical area within a police force also known as an area, borough, division or operational command unit.

Business area
A business area where police information is recorded for a specific policing purpose.

Collection
For the purposes of this guidance, collection refers to the process of obtaining information for a policing purpose. Police information will be collected by routine collection, tasked collection and volunteered information.

Community intelligence
Local information that when assessed provides intelligence on issues that affects neighbourhoods and informs both strategic and operational perspectives in the policing of local communities. Information may be direct or indirect and come from a diverse range of sources including community and partner agencies.

Confidential
The term confidential is used in two different contexts in this document:

1. In line with the Government Protective Marking Scheme (GPMS), accidental or deliberate compromise of assets marked as confidential would be likely to:
   - Prejudice individual security or liberty;
   - Cause damage to the effectiveness of vulnerable security or intelligence operations;
   - Impede the investigation or facilitate the commission of serious crime.
2. Information to which the common law duty of confidence applies.

Confidential information
Confidential information is defined in the statutory Covert Surveillance Code of Practice made under RIPA published in 2001 as:

Confidential information consists of matters subject to legal privilege, confidential personal information and confidential journalistic material.

Confidential personal information
Confidential personal information is defined by section 99 of the Police Act 1997 as:

Information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.

Control strategy
Sets out and communicates the strategic priorities for the force or area.

Covert Human Intelligence Source (CHIS)
A Covert Human Intelligence Source (CHIS) is defined in the Regulation of Investigatory Powers Act 2000, section 26(8), as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of obtaining information or providing access to information to another person or to covertly disclose information obtained by the use of the relationship or as a consequence of the relationship.

Crime and Disorder Reduction Partnership (CDRP)
A statutory partnership in England established by the Crime and Disorder Act 1998.

Crime Reduction Partnership (CRP)
A statutory partnership in Wales established by the Crime and Disorder Act 1998.

Crime series
A crime series is a number of similar crimes which are linked by MO, intelligence or forensic evidence as probably having been committed by one offender or group of offenders.

Data
Data is a subcategory of information and generally refers to information which has been processed on a computer or 'structured filing system'. The Data Protection Act 1998 regulates how personal data is processed. For the purposes of the Act, processing personal information includes:

> 'obtaining, recording, holding and carrying out any operation on the information; organising, adapting, altering; retrieving, consulting, using; disclosing by transmitting, disseminating or otherwise making available; aligning, combining, blocking, erasing or destroying.'

Data Controller
Data controller is defined in the Data Protection Act 1998 as the individual within an organisation who determines the purposes and the manner in which personal data are, or are to be, processed. In a police force this will be the chief officer.

Data Processor
A data processor is a person who processes data on behalf of a data controller.

Data subject
A data subject is an individual who is the subject of personal information.

DCSF
Department for Children, Schools and Families

Disposal
The removal of information from all police systems, justified through the evaluation and review process, to the extent that it cannot be restored.

DIUS
Department for Innovation Universities and Skills

ECHR
European Convention on Human Rights

Enforcement notice
The Information Commissioner has the power to serve an enforcement notice if he or she is satisfied that a public authority has failed to respond properly to a request for information under the Freedom of Information Act 2001. The notice sets out the steps that the authority must take in order to comply with the relevant requirements of the Act. An appeal against a notice may be made to the Information Tribunal, which may confirm, amend or overturn the notice. In the absence of an appeal, however, if the authority fails to comply with a notice then the Commissioner may apply to a court, which will deal with the matter as a contempt of court. The Information Commissioner may serve an enforcement notice upon a data controller who has contravened or is contravening any of the Data Protection principles.

FOIA
Freedom of Information Act 2000

Government Protective Marking Scheme (GPMS)
The Government Protective Marking Scheme (GPMS) sets out common standards for the protection of sensitive documents and other material, including data held on computer and electronic recording systems, against accidental or deliberate compromise. It defines different security classifications of TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. All protectively marked assets should be physically labelled. For further information see **Appendix 7.**

Handling Codes
Handling codes allow the straightforward reporting of decisions on the suitability or otherwise of exposing certain information to other parties. For further information see **Appendix 2.**

IMPACT
Intelligence Management, Prioritisation, Analysis, Coordination and Tasking – programme to deliver the Police National Database and MoPI.

(ISA) (2) Independant Safeguarding Authority

Information
The term information is used in this guidance to refer to all information obtained, recorded or processed by the Police Service. It includes information which is processed (known as data, including personal data) and information which has been subject to a process of evaluation (known as intelligence).

Information Management System
Any system that holds information, including structured paper records and electronic information, and is searchable.

Information Sharing
Information sharing is the passing or receiving from one police force to another or to any non-police organisation or person.

Information Sharing Agreement (ISA)
An ISA is a contract between organisations who wish to share personal information with each other.

Intelligence
Intelligence in this guidance refers to information that is subject to a defined evaluation and risk assessment process in order to assist with police decision making, see **4 Recording Police Information.**

Intelligence Products
Intelligence products are the information sources that drive the Tasking and Co-ordination process. They provide the information upon which strategic and tactical decisions are made and are derived from data compiled from a combination of analytical techniques and products.

Intelligence Requirement
The intelligence requirement provides direction to intelligence staff, frontline officers and support staff as to the information and intelligence that should be collected in relation to the priorities and crimes/incidents that are not currently priorities, but which show a trend that is of concern and/or constitutes a high risk.

Intelligence system
An intelligence system refers to the holding of information which has been evaluated to have an intelligence value.

Law enforcement agency
For the purpose of this guidance, this is an agency with which the police have an agreement to pass intelligence records to, for example, United Kingdom Border Agency.

MAPPA
Multi-Agency Public Protection Arrangements

MO
Modus Operandi

NCRS
National Crime Recording Standard

NFLMS
National Firearms Licence Management System

NRAC
National Retention Assessment Criteria

NSIR
National Standard for Incident Recording

NSPIS
National Strategy for Police Information Systems

National Information/Intelligence Report (5x5x5)
The national Information/Intelligence Report is the standard form for recording information for potential inclusion onto an intelligence system. The report includes the evaluation of the source, content, priority and handling of the information received.

National Intelligence Model (NIM)
Sets out the key elements to successful application of intelligence principles within law enforcement, see ***ACPO (2005) Guidance on the National Intelligence Model.***

National Strategic Assessment
An ACPO document, produced annually, that evaluates strategic issues facing the Police Service.

PNC
Police National Computer

PND
Police National Database

Person Record
For the purpose of this guidance, a Person Record refers to a record containing the minimum of a person's forename and family name, partial name and any nickname or aliases.

Personal data
Defined in the Data Protection Act 1998 as data relating to an identified or living individual.

Policing
This guidance adopts the definition of policing purposes as outlined in ***ACPO(2005) Code of Practice on Managing Police Information,* Section 2.2.2,** ie, protecting life and property, preserving order, preventing the commission of offences, bringing offenders to justice and any duty arising from statute or common law.

Police Service
For the purposes of this guidance, Police Service includes the National Policing Improvement Agency (NPIA), the Serious Organised Crime Agency (SOCA), Counter-Terrorism Units (CTUs) and all Home Office and non-Home Office police forces.

Potentially dangerous people
A potentially dangerous person is somebody who has not been convicted of, or cautioned for, any offence placing them into one of the three MAPPA categories 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. For further information see ***ACPO (2007) Guidance on Protecting the Public: Managing Sexual Offenders and Violent Offenders,*** **pp 52-55.**

Problem profile
A problem profile is an assessment of a specific problem or series of problems, including criminal activities, threats to public safety and anti-social behaviour. It includes an analysis of the problem with recommendations for intelligence gathering, enforcement or prevention.

Processing
This guidance adopts the Data Protection Act 1998 definition of processing and includes the following: obtaining, recording, holding and carrying out any operation on the information; organising, adapting, altering; retrieving, consulting, using; disclosing by transmitting, disseminating or otherwise making available; aligning, combining, blocking, erasing or destroying.

Prosecuting agency
An agency which has a statutory power for prosecuting particular offences, for example, the Crown Prosecution Service.

Provenance
The ability to determine the reliability and credibility of the source, and the value of the information.

Publication scheme
This is a document that details the classes of information that an organisation will routinely make available under the Freedom of Information Act 2000.

Public authority
A public authority is defined under the Human Rights Act 1998 as 'any person, certain of whose functions are of a public nature', and includes courts and tribunals.

Public Interest Immunity (PII)
Public Interest Immunity applications to a court enable the protection of sensitive material and sources if it can be demonstrated that real harm is likely to result from disclosure.

Record
For the purposes of this guidance, a record is any information which can be written down, audio recorded and/or captured visually.

Recording
Recording refers to the process by which information received is noted in writing, for example, in the case of an intelligence system, information will be recorded on a National Information/Intelligence Report.

Retention
The continued storage of and controlled access to information held for a policing purpose which has been justified through the evaluation and review process.

Review
To examine a person record, held for a policing purpose, and all associated records it is linked to, to ensure there is a continuing policing purpose for holding them, that they are adequate, up to date and not excessive and that all records of personal data comply with the eight principles of the Data Protection Act.

Sanitised
Sanitisation of information occurs when material is removed which explicitly or implicitly identifies a source. It also occurs when identifying details of a data subject are removed.

Sensitive personal data
The Data Protection Act 1998 defines sensitive personal data as information that relates to an individual's racial or ethnic origin, political opinions, religious or other similar beliefs, membership of a trade union, physical or mental health or condition, sexual life, alleged or committed criminal offences, proceedings for any offence committed or alleged to have been committed, disposal or sentence concerning any alleged or committed offences.

Serious harm
A risk which is life threatening and/or traumatic and from which recovery, whether physical or psychological, can be expected to be difficult or impossible.

Sexual or violent offender
Section 327 of the Criminal Justice Act 2003 defines a sexual or violent offender.

Single Point of Contact (SPoC)
The nominated individual within a force who acts as a conduit to other organisations and forces in respect of a given business area.

Strategic assessment
Strategic assessments are the key intelligence products that inform the strategic tasking and co-ordination group by giving an accurate picture of the situation in its area of responsibility, how that picture is changing now and how it may change in the future. It is a longer-term, high-level look at law enforcement issues and will, therefore, include current activities as well as try to provide a forecast of likely developments.

Strategic assessments also identify medium-term and long-term policing issues to determine resource, funding and communication requirements.

Strategic Tasking and Co-ordinating Group
The purpose of the Strategic Tasking and Co-ordinating Group (STCG) operating at Levels 1, 2 and 3 of NIM is to consider the strategic assessment in order to set a control strategy and establish an intelligence requirement for the level at which it is operating. The group also reviews and monitors progress of the control strategy, and maintains links with other levels of activity.

Subject access
This is the term given to the right of any individual under the Data Protection Act to have access to personal data about themselves. The right is subject to exceptions.

Systems assets
Systems assets are the IT and manual systems that enable intelligence-led policing to work and ensure the security of data.

Tactical assessments
Tactical assessments identify short-term policing issues on the priorities outlined in the control strategy. They also identify any potential emerging issues outside of the strategy which require attention, and inform tactical tasking and co-ordinating group meetings. The areas covered include intelligence gathering, enforcement, prevention and performance criteria.

Tactical Tasking and Co-ordinating Group
The tactical tasking and co-ordinating group (TTCG) implements the control strategy by agreeing an acceptable tactical response to the problem at a local or force level.

Target profiles
A target profile is a detailed analysis of an individual or network to enable a targeted operation or intervention against that person or network. It also recommends operational intelligence requirements to secure the information required to implement a tactical response.

Third party
In relation to personal information this means any person other than the data subject, data controller or data processor. For example, an employer seeking information from a data controller about a data subject such as a prospective employee.

Threat Assessment
The UK Level 3 Threat Assessment is the responsibility of the National Criminal Intelligence Service.

URN
Unique Reference Number

ViSOR
Violent Offender and Sex Offender Register

Vetting
This refers to a statutory disclosure regime for pre-employment checks, for example, checks established by Part V of the Police Act 1997.

Vulnerable adult
In the context of this guidance, the following definition of vulnerable adult has been adapted from section 5 of the Domestic Violence Crime and Victims Act 2004:

> A person aged 18 or over whose ability to protect him or herself from violence, abuse or neglect is significantly impaired through physical or mental disability or illness, through old age or otherwise.

Appendix 6

References

References

ACPO (2004) *Code of Practice on Data Protection*. London: ACPO.

ACPO (2005) *Code of Practice on the Management of Police Information*. Wyboston: NCPE.

ACPO (2005) *Code of Practice on the Police National Computer*. Wyboston: NCPE.

ACPO (2005) *Guidance on the National Intelligence Model*. Wyboston: NCPE.

ACPO (2005) *Practice Advice on Core Investigative Doctrine*. Wyboston: NCPE.

ACPO (2006) *Guidance on the National Briefing Model*. Wyboston: NCPE.

ACPO (2006) *Threshold Standards: Guidance on the Management of Police Information*. Wyboston: NCPE.

ACPO (2007) *Guidance on Protecting the Public: Managing Sexual Offenders and Violent Offenders*. London: NPIA.

ACPO (2008) *Freedom of Information Manual of Guidance*, Version 5. London: ACPO.

ACPO (2008) *Guidance on Investigating Domestic Abuse*. London: NPIA.

ACPO (2009) *Guidance on Investigating Child Abuse and Safeguarding Children*, Second Edition. London: NPIA.

ACPO (2009) *Manual of Guidance on Data Protection*. London: ACPO.

ACPO (2010) *Guidance on the Management, Recording and Investigation of Missing Persons*. London: NPIA.

ACPO and HMCE (1999) *Code of Practice on the Recording and Dissemination of Intelligence Material*. Wyboston: NCPE.

ACPO and HMCE (1999) *Manual of Standards for the Recording and Dissemination of Intelligence Material*. London: ACPO.

ACPO, ACPOS, PITO and NPT (2001) *Handling of Protectively Marked Material – A Guide for Police Personnel*. Hampshire: NPT.

ACPO/ACPOS (2002) *Information Systems Community Security Policy*. London: ACPO.

ACPO and HMCE (2004) *Manual of Standards for Covert Human Intelligence Sources*. London: ACPO.

ACPO and HMCE (2004) *National Standards in Covert Investigations Manual of Standards for Surveillance of Investigatory Powers Act 2000*. London: ACPO.

Cabinet Office (2009) *HMG Security Policy Framework* [Internet]. London: Cabinet Office. Available from **http://www.cabinetoffice.gov.uk/spf.aspx** [Accessed 3 February 2010]

Criminal Records Bureau (2010) *Criminal Records Bureau (CRB)* [Internet]. London: CRB. Available from **http://www.crb.homeoffice.gov.uk** [Accessed 3 February 2010]

Department of Health (2010) *Department of Health* (DH) [Internet]. London: DH. Available from **http://www.dh.gov.uk/en/index.htm** [Accessed 3 February 2010]

Every Child Matters (2010) *Vetting and Barring Scheme* [Internet]. Available from **http://www.dcsf.gov.uk/everychildmatters/safeguardingandsocialcare/safeguardingchildren/vettingandbarringscheme/vettingvandbarring/** [Accessed 3 February 2010]

FRANCE. Council of Europe (1950) *European Convention on Human Rights 1950 and its Five Protocols: Article 8 – right to Respect for Private and Family Life*. Strasbourg: Council of Europe.

Home Office (2005) *PNC Code of Practice*. London: Home Office.

Independent Safegauarding Authority (2010) *Independent Safeguarding Authority* [Internet]. Available from **http://www.isa-gov.org.uk/** [Accessed 3 February 2010]

Lord Chancellor (2002) *Lord Chancellors's Code of Practice on the Management of Records Under Section 46 of the Freedom of Information Act 2000* [Internet]. Available from **http://www.foi.gov.uk/codemanrec.pdf** [Accessed 3 February 2010]

Ministry of Justice (2010) *Ministry of Justice* [Internet]. Available from **http://www.justice.gov.uk/** [Accessed 3 February 2010]

PITO (2005) *PNC User Manual Volumes 1 and 2*. London: PITO.

Teachernet (2006) *Teachernet* [Internet]. London: DfES. Available from **http://www.teachernet.gov.uk** [Accessed 3 February 2010]

UNITED KINGDOM. Parliament (1956) *Sexual Offences Act 1956*. London: HMSO.

UNITED KINGDOM. Parliament (1989) *Children Act 1989*. London: TSO.

UNITED KINGDOM. Parliament (1996) *Criminal Procedure and Investigations Act 1996*. London: TSO.

UNITED KINGDOM. Parliament (1996) *Police Act 1996*. London: TSO.

UNITED KINGDOM. Parliament (1997) *Police Act 1997*. London: TSO.

UNITED KINGDOM. Parliament (1998) *Crime and Disorder Act 1998*. London: TSO.

UNITED KINGDOM. Parliament (1998) *Data Protection Act 1998*. London: TSO.

UNITED KINGDOM. Parliament (1998) *Human Rights Act 1998*. London: TSO.

UNITED KINGDOM. Parliament (2000) *Freedom of Information Act 2000*. London: TSO.

UNITED KINGDOM. Parliament (2000) *Regulation of Investigatory Powers Act 2000* (RIPA). London: TSO.

UNITED KINGDOM. Parliament (2003) *Criminal Justice Act 2003*. London: TSO.

UNITED KINGDOM. Parliament (2003) *Sexual Offences Act 2003*. London: TSO.

Appendix 7

Government Protective Marking Scheme

Government Protective Marking Scheme

The government protective marking scheme categorises assets according to the harm that the release of the information could cause. For further information see http://www.cabinetoffice.gov.uk/spf.aspx

The categories are:

TOP SECRET

- Threaten directly the internal stability of the United Kingdom or friendly countries;
- Lead directly to widespread loss of life;
- Cause exceptionally grave damage to the effectiveness or security of the United Kingdom or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations;
- Cause exceptionally grave damage to relations with friendly governments;
- Cause severe long-term damage to the United Kingdom economy.

SECRET

- Raise international tension;
- To damage seriously relations with friendly governments;
- Threaten life directly or seriously prejudice public order or individual security or liberty;
- Cause serious damage to the operational effectiveness or security of the United Kingdom or allied forces or the continuing effectiveness of highly valuable security or intelligence operations;
- Cause substantial material damage to national finances or economic and commercial interests.

CONFIDENTIAL

- Materially damage diplomatic relations (ie, cause formal protest or other sanction);
- Prejudice individual security or liberty;
- Cause damage to the operational effectiveness or security of the United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations;
- Work substantially against national finances or economic and commercial interests;
- Substantially undermine the financial viability of major organisations;

- Impede the investigation or facilitate the commission of serious crime;
- Impede seriously the development or operation of major government policies;
- Shut down or otherwise substantially disrupt significant national operations.

RESTRICTED

- Affect diplomatic relations adversely;
- Cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness or security of the United Kingdom or allied forces;
- Cause financial loss or loss of earning potential, or to facilitate improper gain or advantage for individuals or companies;
- Prejudice the investigation or facilitate the commission of crime;
- Breach proper undertakings to maintain the confidence of information provided by third parties;
- Impede the effective development or operation of government policies;
- To breach statutory restrictions on disclosure of information;
- Disadvantage government in commercial or policy negotiations with others;
- Undermine the proper management of the public sector and its operations.

PROTECT

- Cause distress to individuals;
- Breach proper undertakings to maintain the confidence of information provided by third parties;
- Breach statutory restrictions on the disclosure of information;
- Cause financial loss or loss of earning potential, or to facilitate improper gain;
- Give an unfair advantage for individuals or companies;
- Prejudice the investigation or facilitate the commission of crime;
- Disadvantage government in commercial or policy negotiations with others.