

INFORMATION SHARING WITH PARTNERS

Guidance Manual 2008

Management of Police Information (MoPI)

Produced on behalf of the

Association of Chief Police Officers in Scotland (ACPOS)



Guidance on The Management of Police Information ACPOS Nov 2007

NOT PROTECTIVELY MARKED



This guidance contains processes to assist the police service and partners to ensure consistent information management.

All enquires about this guidance should be addressed to:

The ACPOS NIM Development Project
Scottish Police College
Tulliallan Castle
Kincardine
Fife
FK10 4BE

Telephone: 01259 732082
E-mail: NIM@tulliallan.pnn.police.uk

Acknowledgements

ACPOS would like to express their thanks in the completion of this document to ACPO and the NCPE (now NPIA) for allowing the ACPO (2005) Guidance on the Management of Police Information to be adapted to suit the Scottish context.

© Association of Chief Police Officers (2006)

© Centrex (2006)

All rights reserved. No part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of NPIA and ACPOS or their duly authorised representative.

CONTENTS

Preface	6
Section 1 THE PURPOSE OF MANAGING POLICE INFORMATION	7
1.1 What Is This Guidance?	8
1.2 What Is Police Information?	8
1.3 Information As A Resource For Policing	9
1.4 Legal Basis For Managing Police Information	10
1.5 Chief Officer	18
1.6 Stages Of Managing Police Information	12
Section 2 THE PROCESS FOR MANAGING POLICE INFORMATION.....	13
2.1 Need For Common Processes	14
2.2 Records Management.....	14
2.3 Business Areas For Managing Information.....	15
2.4 Critical Information Areas.....	15
2.5 Information Management Strategy.....	17
2.6 Responsibilities	18
2.6.1 All Staff	19
Section 3 COLLECTION OF POLICE INFORMATION	21
3.1 Why Police Information Is Collected	22
3.2 How Police Information Is Collected	22
3.3 Responsibilities	23
3.3.1 Managers	23
3.3.2 Supervisors	23
3.3.3 Users.....	23
Section 4 RECORDING POLICE INFORMATION.....	25
4.1 Why Recording Information Is Important	26
4.2 Principles Of Recording	26
4.3 How Police Information Is Recorded?.....	27
4.4 Data Quality Principles.....	27
4.5 Nominal Records.....	28
4.6 Responsibilities	30
4.6.1 System Owners.....	30
4.6.2 Managers	30
4.6.3 Supervisors	30
4.6.4 Users.....	31
Section 5 EVALUATION AND ACTION OF POLICE INFORMATION	33
5.1 Why Evaluate Police Information?	34
5.2 Principles of Evaluating Police Information.....	34
5.3 How Police Information Is Evaluated	35
5.4 Action Management	35
5.5 Responsibilities	36
5.5.1 Managers	36
5.5.2 Supervisors	36
5.5.3 Users.....	36

CONTENTS

Section 6	INFORMATION SHARING	37
6.1	Why There Is A Need To Share Police Information	38
6.2	Information Sharing Landscape	39
6.3	Statutory Obligation	39
6.3.1	Disclosure Under Part V Of The Police Act 1997	39
6.3.2	Notifiable Occupations Scheme	40
6.3.3	Schemes To Protect Children And Vulnerable Adults	40
6.3.4	Disclosure Under The Freedom Of Information (Scotland) Act 2002	41
6.3.5	Disclosure Under The Data Protection Act 1998	41
6.4	Statutory Power	41
6.4.1	Other Types Of Sharing Where A Statutory Power Exists	43
6.5	Common Law	43
6.5.1	Dissemination Of Intelligence	43
6.6	How The Police Share Information	44
6.6.1	Police Information Must Be Accurate	44
6.6.2	Police Information Must Be Judged On Its Own Merits	45
6.6.3	Relevance Should Be Clearly Explained	45
6.7	Considerations When Sharing Personal Information	45
6.7.1	Proportionality	46
6.7.2	Data Protection Act 1998	46
6.7.3	Common Law Duty Of Confidence	47
6.7.4	Disclosure Of Restricted Or Confidential Material To Third Parties	47
6.8	Sharing Through An Information Sharing Protocol	49
6.8.1	Establishing A Purpose For The Creation Of An Information Sharing Protocol	51
6.8.2	Consent And The Data Protection Act 1998	51
6.8.3	Setting Out The Process For Sharing Information	52
6.8.4	Sharing Within An Information Sharing Protocol	54
6.9	Review	55
6.9.1	Is The Agreement Still Useful And Fit For Purpose?	55
6.9.2	Does The Information Sharing Protocol Have The Correct Contact List?	55
6.9.3	Is The Agreement Still Useful And Fit For Purpose?	56
6.10	The Process Of Sharing Police Information Outwith The Terms Of An Information Sharing Protocol	56
6.11	Responsibilities For Managing Information Sharing	57
6.11.1	Managers	57
6.11.2	Supervisors	57
6.11.3	Users	57

Section 7	RETENTION, REVIEW AND DISPOSAL	59
7.1	Legal Issues	60
	7.1.1 Human Rights Act 1998	60
	7.1.2 Data Protection Act 1998	60
	7.1.3 Freedom Of Information (Scotland) Act 2002	60
7.2	Retention	61
	7.2.1 Duplication	62
	7.2.2 Productions	62
	7.2.3 Storage And Preservation	62
7.3	Why Review Police Information	63
7.4	Historical Data	63
7.5	Disposal	63
	7.5.1 Recording Disposal	64
	7.5.2 Method For Disposal	64
7.6	Audit Of Retention, Review And Disposal	64
7.7	Responsibilities	65
	7.7.1 System Owners	65
	7.7.2 Managers	65
	7.7.3 Supervisors	65
	7.7.4 Users	65
Appendix 1 - ISP Template / Example		67
Appendix 2 - GLOSSARY		75
Appendix 3 - REFERENCES		87
Summary of Checklists		
	Checklist 1: Recording Police Information	31
	Checklist 2: Sharing Police Information	44
	Checklist 3: Sharing Police Information Outside an ISP	64
Summary of Figures		
	Figure 1: Information Sharing Protocol (ISP) Process Chart	50

PREFACE

This guidance on the Management of Police Information has been developed for the Association of Chief Police Officers for Scotland. It is derived from the similar document produced by the National Centre for Policing Excellence on behalf of the Association of Chief Police Officers for England and Wales following the publication in July 2005 of the associated code of practice. The code of practice formed part of the government response to recommendations made by Sir Michael Bichard following the inquiry into the circumstances around the murders of Jessica Chapman and Holly Wells in Soham by Ian Huntley.

ACPOS has endorsed the adaptation of the ACPO guidance manual as the Scottish framework for the management of police information, a key element of which is the defined need for common standards in high risk areas of activity.

This guidance gives definition to the term policing purposes in terms of information management. Policing purposes have deliberately been described at a high level and are intended to be inclusive. The definition does not incorporate every policing activity and no existing legal power or duty on the police is superseded. The fact that these policing purposes do not specifically refer to an activity, e.g. roads policing, protection of vulnerable persons or counter-terrorism, does not in any way imply that these are not legitimate activities for the purposes of police information management. It is important to distinguish between information that is collected for a policing purpose which is covered by the guidance, i.e. the six identified key priority areas and information ancillary to a policing purpose, e.g. personnel, pay or invoice records which are not covered and will be dealt with in future phases.

This guidance is subject to a nationally agreed implementation strategy, the oversight of which lies with the ACPOS NIM / MOPI Development Project. This involves the attainment of associated threshold standards which will be subject to a phased implementation. These standards sit outside the guidance itself but are part of the overall package for Chief Officers to take account of in terms of police information management.

The phased implementation of the guidance on the Management of Police Information recognises the challenge for the Scottish police service at this time. The focus of this activity in the initial phase will be on the following six areas which are considered to present the highest threat and risk to the service in terms of information management:

- Crime
- Intelligence
- Domestic Violence
- Child Abuse Investigations
- Firearms Revocations and Refusals
- Custody

The emphasis for the first phase will be on the standards relating to infrastructure, policy, processes and procedures. Further phases are likely to follow which will progressively raise standards across the whole area of police information management, subject to understanding the full impact across the police service.

The guidance may necessarily require a thorough review following the service experience resulting from implementation.

Compliance for the initial phase will be timetabled in the latter part of 2007 once force and SCDEA capability assessments have been considered by ACPOS.

Section 1

THE PURPOSE OF MANAGING POLICE INFORMATION

This section describes what is meant by police information and why it is a key resource for the police service. It also provides an outline of the legal basis for police information management and the stages involved in managing it.

Key principles of this section are that:

- Police information is information for a policing purpose.
- Police information must be managed lawfully.
- Information is a corporate resource for the police service.

1.1 WHAT IS THIS GUIDANCE?

This guidance sets out a framework for the management of police information based on the principle that effective policing is dependent on efficient information management. As such the guidance is based on considerable 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 will meet key recommendations of the Bichard Inquiry which relate to police information management.

This guidance replaces the following which were previously applicable in Scotland:

- *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) Manual of Standards for the Recording and Dissemination of Intelligence Material.*

All other guidance relevant to the management of police information remains valid. Specific links between this and other guidance is indicated in the text. For additional information there is benefit for those in key posts referring to the ACPO Code of Practice on the Management of Police Information 2005.

1.2 WHAT IS POLICE INFORMATION?

For the purposes of this guidance police information is information that is required for a policing purpose. Policing purposes are defined as:

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

These five policing purposes provide the basis for collecting, recording, evaluating, sharing, retaining and destroying police information. The policing purposes do not replace or supersede any existing duty or power defined by statute or common law. The policing purposes do not therefore, define every policing activity, and the fact that these are not set out does not mean that there is no legal basis for performing the activities. For example, information relating to such key policing functions such as roads policing, public order, counter-terrorism or protection of children and other vulnerable groups, while not referred to explicitly are, nonetheless, legitimate policing functions requiring information.

The five policing purposes are not mutually exclusive. Information can be collected for one policing purpose and used for another that may not have been known about at the point of collection. It is essential that a policing purpose is established in order for information to be legally held.

Policing is a continuous risk management exercise. It is, therefore, essential that the processes for managing police information focus on managing the risk attached to that information. This can be done both by ensuring that there are clear and consistent processes for collecting, recording and evaluating police information, and that effective processes are in place to take appropriate action on the basis of it. Later sections of this guidance discuss this in more depth.

Effective intelligence management is at the heart of police information management. Intelligence is defined as information that is subject to a defined evaluation and risk assessment process in order to assist with police decision making.

The defined evaluation and risk assessment process is that obtained by adopting the 5x5x5 principles, along with any required additional risk assessment, which will meet the required needs of source protection. Police decision making, in this context, is founded upon the development of intelligence to direct future action. Adopting this definition of police information ensures that all information is considered in terms of this guidance, and not just that which is evidence.

Intelligence management involves linking together information from a wide range of sources - from open source and publicly available information to that obtained covertly in order to build up a composite picture. This will highlight links between people, objects, locations and events that are essential in supporting the policing purposes described. Identifying these 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), which has been adopted as the common business process for policing in the UK.

NIM is dependent on information to feed the intelligence process. The implications of this on the way in which information is managed are described in more detail in [2 The Process for Managing Police Information](#), and the *ACPOS (2006) Guidance on National Intelligence Model*.

1.3 INFORMATION AS A RESOURCE FOR POLICING

Collection of the appropriate information, its accurate assessment and timely exploitation, are core to efficient policing.

Information that is collected for one policing purpose may have a value to another. For this to happen all police information must be treated as a corporate resource. Information collected in one area command / division within a force or agency may be relevant to another area command / division, another force or agency.

It is, therefore, important 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 and, if it has a policing purpose, it should not matter where the information originated from but should be available to support that policing purpose.

Information has, however, been traditionally held in business areas that are not connected and are not capable of being searched. This has meant that it has been difficult to link together people, objects, locations and events, even within the same force / agency. This situation is exacerbated across Scotland because of a lack of common standards for information recording and evaluation. This means that sharing information within the police service and with key partners can be unnecessarily complex.

The process for ensuring that police information is a corporate resource at both force and national level is described in section 2 [The Process for Managing Police Information](#).

This guidance provides a definition of UK national standards for police information management to support the establishment of a common information infrastructure for policing. The IMPACT programme is currently developing a capability in England and Wales for the police service to link together people, objects, locations and events across force boundaries to provide a national information resource. That programme will be underpinned by the ACPO guidance on the Management of Police Information. The Scottish police service is engaged with the IMPACT programme through the roll out of the IMPACT Nominal Index (INI) in Scotland.

For further information on the IMPACT programme see,

<http://www.pito.pnn.police.uk/microsite/impact/>

1.4 LEGAL BASIS FOR MANAGING POLICE INFORMATION

In order for police information to be made available to support policing purposes the legal framework must first be understood. This guidance does not set out the detail of the legal framework, but the key principles that must be satisfied for police information to be managed lawfully. It should be emphasised that compliance with the law cannot be ignored because it is inconvenient; compliance is central to the management of police information.

Achieving legal management of police information involves a number of stages. The stages are summarised below and apply to all the phases of the information management cycle which are described in detail in this guidance.

Establishing a policing purpose

Establishing a policing purpose is the cornerstone of effective management of police information. If the information can be shown to meet a policing purpose then the legal basis for holding it can be established. Without this, the information cannot be held as police information.

The Police (Scotland) Act 1967

The Police (Scotland) Act 1967 establishes the legal basis for the functions of the police in Scotland. This provides clear guidance on the duties and powers of a constable.

Implications of The Scotland Act 1998

The Scotland Act 1998 incorporated most of the European Convention on Human Rights (ECHR) into Scottish legislation. The ECHR contains a number of fundamental rights which have a bearing on the management of police information. The Scotland Act 1998 makes it unlawful for a public authority, including a police force / agency, to act in a way that is incompatible with 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 inhumane or degrading treatment (Article 3). Article 8 of the ECHR protects an individual's right to privacy and family life. This right is not absolute but may not be interfered with except in accordance of the law; in pursuit of a legitimate aim; and necessary in a democratic society. This places a responsibility on police forces to set a clear aim for obtaining personal information (a policing purpose) and a test of proportionality of how they meet this aim.

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) and the Regulation of Investigatory Powers (Scotland) Act 2000 RIP(S)A.

Is the police information personal data?

Once the policing purpose is established the issue arises regarding whether the information is covered by the Data Protection Act 1998 (DPA). If the information is personal or sensitive personal data then, under 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 or data in the possession of the Data Controller. Much police information is covered by the DPA, and is referred to in this guidance as personal information.

What does the Data Protection Act 1998 require?

The DPA requires personal information to comply with the eight data protection principles:

- Being fairly and lawfully processed;
- Being processed for limited 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 being transferred to countries outside the EEA without adequate protection.

The DPA also requires information to be made available to the subject of that information at their request, with certain exemptions.

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.

What exemptions are there from the Data Protection Act 1998?

There are a number of exemptions from the DPA including section 28 (national security), section 33 (research and statistics), and section 35 (legal proceedings).

Particularly relevant to police information is section 29 which creates exemptions to certain DPA 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 must be applied on a case by case basis and cannot be used to justify routine data processing. The advice of DPA staff and legal services is available and recommended should further information be needed. Additional information on the implications of the DPA is available at <http://www.dca.gov.uk> or <http://www.ico.gov.uk> and *ACPO (forthcoming) 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. These stages are covered in detail in subsequent sections and are summarised here:

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

Section 2

THE PROCESS FOR MANAGING POLICE INFORMATION

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, is described here.

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 is a link between police information that is held in different business areas. This will 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 / agency.

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, for a different purpose. This requires consistent processes to be in place at all levels of policing activity in order to manage police information as a corporate resource for the police service as a whole.

At ACPOS level and force / agency level, there is a need to amend processes to allow information to be linked and composite records to be maintained as a corporate resource. This means that every force / agency must know what information it holds, where and how it holds it and that it can, when required, provide such details to ACPOS. This is particularly important for ICT system specification purposes. Technology is dependent on consistent processes to be in place and adhered to, therefore national ICT systems cannot be developed without the prior agreement of common processes and data standards. In Scotland progress has been made in this area through the implementation of the Scottish Intelligence Database (SID). As other national systems are developed they will be designed to allow common processes to be utilised, i.e. crime recording. This guidance does not specify any technical solutions to 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 must be in a format that is manageable, irrespective of the format and media in which it is held.

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 life cycle from creation to disposal. This process will involve the audit and maintenance of records to enable them to remain useful for a policing purpose. This will also enable the discharge of legal responsibilities outlined in [section 1 The Purpose of Managing Police Information](#).

Records should be managed in line with the [ACPOS Records Retention Schedule](#), the [Freedom of Information \(Scotland\) Act 2002, Section 61](#) and force / agency policies and procedures.

2.3 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 individuals in custody will be held on a custody system. It is important, however, that a record stored in one business area can be linked to a record in another one.

The six identified key business areas in this phase of implementation are managed via relevant information systems which hold police information that will contain particularly significant records for policing purposes. These include, but are not limited to:

- Crime Recording;
- Domestic Violence;
- Child Abuse Investigation;
- Public Protection;
- Missing Persons;
- Case and Custody;
- Command and Control;
- Firearms Licensing;
- Intelligence;
- SCRO Criminal History System.

These various business area information systems will have distinct criteria for how information is recorded on them, e.g. the Scottish Crime Recording Standard. These criteria must support the fundamental principle that the information held on any police information system is capable of being cross-referenced against information held by other police business areas.

2.4 CRITICAL INFORMATION AREAS

Some police information will be particularly valuable to policing. No guidance can prescribe exactly the type of police information that will be critical in any given circumstance; that decision can only be made by staff in possession of the relevant facts.

The NIM has a significant bearing on determining critical police information. Strategic assessments at national / force / agency and area command / divisional level inform the setting of a control strategy identifying overall risk areas for policing and defining particular priorities at those levels. The control strategy should inform the setting of an intelligence requirement that identifies specific information needs, depending on local circumstances.

There is certain information however, that should always be considered. This includes:

- Information about threats to life or of serious harm;
- Information about known or suspected offenders;
- Information obtained from sensitive or covert sources; and
- 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 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 *ACPOS (2006) 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 human rights legislation under ECHR, particularly in relation to Article 2 (Right to Life) and Article 3 (the right not to be subjected to inhumane or degrading treatment). Forces / agencies, therefore, must have specific arrangements in place to manage information relating to public protection. There are classes of information which are critical to efficient public protection arrangements, described as 'certain public protection matters'. Certain public protection 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 serious crime enquiries. See [Appendix 2: Glossary](#).

- Information relating to Potentially Dangerous People – Individuals who have not been convicted of any offence of a sexual or violent nature and who does not fall within any of the MAPPA categories. Their behaviour, however may give reasonable grounds for believing that there is a real likelihood of committing an offence or offences likely to cause serious harm.

For further information see *ACPO (forthcoming) Guidance on Public Protection*. For further information on reviewing and retaining information which includes that related to certain public protection matters, see [Section 7: Retention, Review and Disposal](#).

2.5 INFORMATION MANAGEMENT STRATEGY

The previous sections 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 / agency must first be defined in a force / agency Information Management Strategy (IMS). An IMS must be developed within each force / agency and maintained under the responsibility of a chief officer. Each force / agency IMS should be aligned to this guidance and the accepted threshold standards for the management of police information. The MOPI guidance will act as the National IMS.

The IMS will be a high level document which sets out the principles applying to information management within the force / agency. 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 will identify the information community within the force / agency and define the processes for managing information within the force / agency and with partners. It will allow information to be exploited wherever it is needed within the force / agency, and define how barriers can be overcome. The IMS will set out the following:

- Who is responsible for police information held within the force / agency.
- The purposes for collecting and holding information.
- Which business areas will be holding information within the force / agency, and the standards that will apply within those areas.
- The safeguards that will be applied to police information held by the force / agency.
- 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 confidentiality, integrity and availability of police information held by the force / agency in terms of information assurance.
- The training that will be in place to support the management of police information.
- The dedicated resources that will be 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 / agency will comply with national and local security policy and standards.
- How information will be shared through the use of Information Sharing Protocols (ISPs).
- The process for sharing information under ISP's.
- How information will be destroyed and how the reason for destruction will be recorded.
- How information will be audited.

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, retention and disposal of police information. There are a number of core responsibilities, however, that need to be in place centrally in order to support effective information management. This section defines these responsibilities, but they should not be seen as additional requirements on forces / agencies to those that have already been implemented for the NIM. These responsibilities are complementary to those outlined in the people assets section in the *ACPOS (2006) Guidance on the National Intelligence Model*. Functions that are already in place may be adapted to include the responsibilities required for managing police information.

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

Appendix 1 in *ACPO (2006) Threshold Standards for the Management of Police Information*, that complements this guidance, defines suggested roles and functions in greater detail and may be of use to forces / agencies as a reference document when defining MOPI related responsibilities.

2.6.1 CHIEF OFFICER

The chief officer has overall responsibility for a force / agency's implementation of this guidance. The chief officer will own the IMS and have responsibility for ensuring that force / agency policies and processes are compliant 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 / agency. Such a role would be accountable to the chief officer for the everyday management of police information within the force / agency.

A number of forces / agencies have already followed good practice by appointing a Chief Information Officer at senior management level to oversee information management within the organisation.

2.6.2 ALL STAFF

All police staff are involved in the management of police information. As such, they will have specific responsibilities according to their role as detailed within each section of this guidance. In addition, the following responsibilities apply to all staff, to:

- Apply the basic principles of effective information management as contained within this guidance.
- Ensure staff act within the framework of the force / agency IMS and associated force / agency policies and processes.
- Apply data quality principles to all police information as set out in [Section 4: Recording of Police Information](#).
- Apply operating rules relevant to 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 (Scotland) Act 2002.

For definition of police staff see [Appendix 2 - Glossary](#).

For further information in relation to responsibilities see [Appendix 1](#) in *ACPO (2006) Threshold Standards for the Management of Police Information*.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Section 3

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.

3.1 WHY POLICE INFORMATION IS COLLECTED

The collection and recording of police information is key to effective policing (see [Section 1.2: What is Police Information?](#)).

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, correctly and consistently. This stage should not be seen in isolation and will affect all other stages of information management from how to record the information to how long it will be retained for.

The principles and standards of a police information management strategy (IMS) must apply from the point of collection. A force / agency IMS will allow for information requirements to be set and therefore determine what information should be collected. The IMS will support force / agency and area command / divisional level intelligence requirements, as a dynamic process in accordance with the NIM. These support service delivery and determine business needs through identified national and force / agency / 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 use to inform business management and statistical processes. The collection and subsequent recording and evaluation of police information allows areas of risk to policing business to be identified, prioritised and actioned.

The means of collection of information will be relevant to how the information should be processed. For example, there is a distinction between information that is volunteered and that which is gathered covertly. In some circumstances, the way in which police information is collected may lead to specific requirements as to its recording and use.

3.2 HOW POLICE INFORMATION IS COLLECTED

Police information is collected in a number of different ways but the majority is passed to the police service through traditional methods, for example, the public reporting of an incident or crime. The adoption of intelligence led 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 as part of general operational policing activity;
- Tasked information for a specific purpose; or
- Volunteered information from members of the public, community contacts and partners.

3.3 RESPONSIBILITIES

The guidance sets out the responsibilities of managers, supervisors and users in this section as follows:

3.3.1 MANAGERS

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

3.3.2 SUPERVISORS

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

3.3.3 USERS

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

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Section 4

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 will be 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.
- Police information held in different business areas should be inter-linked.

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 where it then becomes available to all.

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 held for a policing purpose is in accordance with the law.
- The ability for the information to support decision making through the 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.
- The establishment of corporacy and governance processes in relation to information management ensuring confidentiality, integrity and availability.

Failure to record information correctly can prevent forces / agencies from being able to adequately manage risk to the public, create a potential misuse of resources and not meet national and local policing objectives. It is essential, therefore, that data standards in use across Scotland are adhered to.

4.2 PRINCIPLES OF RECORDING

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

- Records can exist in any format. They can be written, electronic, audio recorded and / or captured visually for example CCTV, photographs etc.
- All records must comply with the data quality principles in [Section 4.4](#).
- A record of police information is the start of an audit trail and must identify who completed the record, when it was completed, amended, edited and for what purpose.
- Before recording information, checks must be made in other business areas to see whether this information is already held elsewhere to avoid unnecessary duplication.
- 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 must first be given to any sensitivities in recording it to ensure that it is given 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.
- ACPOS approved metadata standards should be observed.

4.3 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. (See examples in [Section 2.3](#)) These include, but are not limited to:

- Crime recording
- Domestic violence
- Child abuse investigation
- Public protection
- Missing persons
- Case and Custody recording
- Incident records
- Firearms licensing
- Intelligence
- Criminal History System recording

Police business requires information to be linked together within forces / agencies and across force / agency boundaries. Successful links can only be achieved through standard business processes, high levels of data quality and common standards.

The IMS should specify where information is recorded. It is a requirement of the DPA that business areas which contain personal data are notified to the Information Commissioner. For further information see [ACPO \(forthcoming\) Manual of Guidance on Data Protection](#).

4.4 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 get it right at the outset could lead to further work and an increased likelihood of missing a potentially vital link. High quality information helps to ensure that appropriate action is taken, that information is shared where possible, and that it can be retained for the appropriate period of time.

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 which may be significant e.g. 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 (clearly more information will be necessary from a witness to a fatal incident than a minor road traffic incident). 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.

4.5 NOMINAL RECORDS

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

Nominal records are of greatest importance and value to the police service, making their recording and subsequent use and management a priority when managing police information. However, they present the most risk for offenders, victims, witnesses and sources. It is essential that nominal information is processed appropriately to meet all legal obligations in terms of DPA.

Data quality is essential in the creation of nominal records in order to ensure the proper management of records throughout their life across all business areas. This allows effective linking of information which can be searched and used for policing purposes. The risk and threat attached to poor or ineffective data quality management may result in serious offenders not being identified through information management processes. The potential consequences of this are self evident. By recording in greater detail, increases the likelihood that the nominal record will be unique. This must, however, be proportionate to the reason for recording the information.

For the purpose of this guidance the creation of a nominal record will contain as a minimum a person's forename and family name and, where known, their nickname or alias. A description without a name attached will not lead to the creation of a nominal record.

NOT PROTECTIVELY MARKED

A key desirable element for effective identification of nominals is clearly the date of birth and this should be obtained on all occasions where it is possible to do so. Certain key business areas where nominal records are created have specific criteria for the creation of such nominals and reference should be made to the SOP for that business area in this matter. This will include *ACPOS SID Rules, Conventions and Data Input Standards (Version 6) June 2006* and Scottish Criminal Records Office (SCRO) Criminal History System (CHS) policy etc. Other desirable basic fields to include on a nominal record are:

- Gender
- SCRO / PNC ID number or numbers
- National Insurance Number
- Colour / Ethnicity
- Full Postal Address or a Meaningful Partial Address
- Communications information e.g. Internet ISP, telephone / fax numbers
- Employment Details
- Vehicle registration number

In order to create a nominal record every effort should be made to confirm a person's identity. This is important to avoid duplication of nominal details contained in systems through variation in recording of the specific details. Police have the power under Section 13 of the Criminal Procedure (Scotland) Act 1995 as introduced by Section 81 of the Police, Public Order and Criminal Justice (Scotland) Act 2006 to require suspects for, and / or witnesses to, a crime or offence, to provide the following information in addition to his / her name and address:

- Date of birth;
- Place of birth (in such detail as the officer considers necessary for the purpose of establishing the person's identity); and
- Nationality.

Section 81 of the Act also amends Section 14 of the Criminal Procedure (Scotland) Act 1995 in relation to detained persons, and places an obligation on a person so detained to provide the police with the same additional information. It is important that a person's date of birth is recorded where it is known or can be obtained and, if necessary, the appropriate power must be used to obtain such information.

Establishing a unique reference number (URN) which can be linked to a nominal record is a vital factor in the organisation of information. This referencing allows information to be managed more effectively both at force / agency and national level, and enables effective linking of relevant nominal data.

The SCRO CHS and Police National Computer (PNC) are sources which can help confirm a person's identity. Checks should be made to establish whether a person is already known to the police. Name checks on these systems alone should not be the only method of verification and cannot be relied on solely for correct identification. Where possible, biometrics such as fingerprints and other information, including marks and scars, should be used to help confirm identity. If a CHS or PNC record can be accurately linked to a nominal record then a cross-reference should be made on the appropriate databases through the relevant URN.

The release of the Impact Nominal Index (INI) as the first phase of IMPACT delivery creates a capability to search nominal records nationally. The way in which this is further managed will change with the development of IMPACT.

For further information on the IMPACT programme see,

<http://www.pito.pnn.police.uk/microsite/impact/>

4.6 RESPONSIBILITIES

The guidance sets out the responsibilities of managers, supervisors and users in this section as follows:

4.6.1 SYSTEM OWNERS

- Both nationally and locally are responsible for system audits.
- Ensure that local systems meet national standards.
- Undertake compliance checking.

4.6.2 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 appropriately.

4.6.3 SUPERVISORS

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

4.6.4 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 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.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED

Section 5

EVALUATION AND ACTION OF POLICE INFORMATION

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

Key principles of this section are that:

- 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.

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, particularly that which comes from intelligence, is evaluated to determine its provenance, accuracy, continuing relevance to a policing purpose and any action to 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 point in time, subject to review.

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 progress requiring a more immediate response than a report of an abandoned vehicle). 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 of these incidents being entered onto an information / intelligence report.

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

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 content must 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.
- Links must be identified between different records.
- Information will be assessed for its intelligence value and its input into the intelligence business area if appropriate.
- 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 [Section 5.2: Principles of Evaluating Police Information](#) specific evaluation criteria apply to the following business areas:

- Crime recording
- Domestic violence
- Child abuse investigation
- Public protection
- Missing persons
- Case and custody
- Incident records
- Firearms licensing
- Intelligence

5.4 ACTION MANAGEMENT

Evaluating information enables priorities to be identified and the appropriate action taken. This action management process is the means of identifying where there are risk factors that require an immediate response, for example, a threat to life or significant risk to the public.

Actioning any police information will result 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 the decision not to do anything at this point in time, but subject to review at a future date.
- Intelligence material will be the subject of priority assessment as part of the action management process.

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

For further guidance on the decision making process, see [ACPOS \(2006\) Guidance on The National Intelligence Model](#).

5.5 RESPONSIBILITIES

The guidance sets out the responsibilities of managers, supervisors and users in this section as follows:

5.5.1 MANAGERS

- Ensure that all information management processes are robust, reliable and relevant.
- Follow the principles of the NIM.
- Ensure that information is priority assessed.
- Ensure that the staff responsible for evaluating police information are trained appropriately.

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 relevant and 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 together of information where relevant.
- Identify opportunities for analysis of series or linked events.
- Apply provenance to the information recorded where relevant.
- Apply relevant priority assessment if appropriate.
- Disseminate information where appropriate.

Section 6

INFORMATION SHARING

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

Key principles of this section are:

- The need to protect the public and our common law duty of care can require that information be shared within the service, with partner agencies and the public**
- Police forces should actively seek opportunities to share anonymous (i.e. non personal) information within the context of audit arrangements as a precursor to creating joint strategies and operational action plans in support of statutory responsibilities, for example Community Plans, Behaviour Strategies and Child Protection Strategies created under the umbrella of Children's Services responsibilities.**
- Establishing a policing purpose or other legal gateway, including the exceptions to the Duty of Confidentiality, is the basis for sharing police information.**
- Information sharing arrangements (through MOUs or Protocols) between the police and partner agencies should be used to ensure consistent and proportionate sharing of information and should be reviewed and audited on a regular basis.**
- Any decision to disclose police information must adhere to the principles of the Data Protection Act 1998.**
- The need for Police staff to receive appropriate training to enable them to share information within the current legislative framework.**

6.1 WHY THERE IS A NEED TO SHARE POLICE INFORMATION

Information sharing is generally taken to mean the ongoing use of data, which may or may not be personal data, by the public sector, across traditional organisational boundaries, to achieve better policies and deliver better services for individuals and society as a whole. Disclosure includes merely using or making available personal data within an organisation but the term also includes transmission of such data to other parties outside the original processing agency.

Effective policing relies on the police service communicating and sharing information with a wide range of partners. Information sharing therefore:

- Is a two-way process that enables links to be made between people, objects, locations and events that would not be possible otherwise.
- Can help deliver improved public services, leading to improved well-being for citizens.
- Leads to an openness among partners, which in turn, builds confidence and trust in the service.
- Increases expertise, professionalism and an understanding of the process of sharing information.
- Leads to informed decisions being taken within a multi-agency setting thereby improving outcomes for individuals and communities (including the individual whose personal data is being disclosed).
- Enables effective joint problem solving.

However while there are clear advantages in sharing information with others, information should not be shared purely as a matter of routine. Each case must be reviewed 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. For a more comprehensive guide to data sharing please refer to “Data Sharing: Legal Guidance for the Public Sector (www.scotland.gov.uk/Topics/Government/Open-scotland) and the Office of the Information Commissioner (www.informationcommissioner.gov.uk).

In situations where complex individual queries are encountered advice should always be sought from police staff within Legal Services, Information Security, Disclosure or Freedom of Information units and Data Protection Officers.

6.2 INFORMATION SHARING LANDSCAPE

The sharing of police information can be summarised in three distinct groups:

- That required by or under statute (statutory obligation);
- That permitted by or under statute (statutory power – an example of which is Section 139 of the Behaviour etc. (Scotland) Act 2004 which provides a legal protection for those who disclose information where it is necessary or expedient for the purposes of preparing to apply for an Behaviour order or any other provisions contained within the Act); and
- That made under common law to support policing purposes, including dissemination and particularly where there is an overriding public interest (i.e. where the benefits to an individual or to society of the disclosure outweigh the public and the individual's interest in keeping the information confidential.) An example of this would be disclosing personal data to the media including an image in relation to someone where there is knowledge of a stated intention allied to a capability to cause serious harm to himself or to others.

Further detail on these categories can be found in [Sections 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:

- The Notifiable Occupations Scheme.
- Disclosures to the Child Support Agency and the Scottish Criminal Records Office,
- Section 53 of the Children (Scotland) Act 1995 which requires a police officer to refer a child to the Reporter where there is reasonable cause to believe that compulsory measures of care may be required.
- The Protection of Children (Scotland) Act 2003 in relation to the list regarding those disqualified from working with children.

Where there is a frequent and continuing need for the police service to disclose information a memorandum of understanding (MOU), information sharing protocol (ISP) or service level agreement (SLA) which clearly sets out the statutory obligations of the organisations involved, together with the procedures for managing them, should be used to ensure effective, timely and consistent disclosure.

Key schemes where the police service is obliged to disclose personal data are detailed in [Sections 6.3.1 to 6.3.5](#)

6.3.1 DISCLOSURE UNDER PART V OF THE POLICE ACT 1997

Part V of the Police Act 1997 creates a statutory scheme for the disclosure of criminal records and other relevant police information on potential employees to prospective employers. Disclosure Scotland is responsible for the scheme in Scotland (the Criminal Records Bureau in England and Wales) and for ensuring that employers have sufficient information to make a judgement on the suitability of a potential employee when working with children or vulnerable adults.

Following on from Recommendation 20 of the Bichard Report forces will shortly introduce a Quality Assurance Framework (QAF) to help to ensure consistency in the decision making processes for the disclosure of information by the police to Disclosure Scotland. This will be done by:

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

Further information is available at www.disclosurescotland.co.uk

6.3.2 NOTIFIABLE OCCUPATIONS SCHEME

The Notifiable Occupations Scheme relates to professions or occupations that carry special trust or responsibility in which 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. The Notifiable Occupation Scheme will need to remain in Scotland following the enactment of the (forthcoming 2007) Protection of Vulnerable Groups (Scotland) Bill for those occupations to which it currently applies and which will not be included within the vetting and barring scheme. It will also have a continuing role in ensuring that employers are made aware of all convictions even where these might not be relevant to the protection of vulnerable groups.

Notwithstanding this under Police Circular CC: 4/89 the Chief Constable retains the right to disclose sensitive personal information in relation to those notifiable occupations detailed in the relevant annex.

6.3.3 SCHEMES TO PROTECT CHILDREN AND VULNERABLE ADULTS

The Scottish Executive Education Department currently operates the Protection of Children (Scotland) Act 2003 list (known as the Scottish Disqualified from Working with Children List or DWCL) which contains details of people who are known to be unsuitable to work with children in childcare positions. This list refers to people who are not allowed to be employed by educational institutions as a teacher or in work involving regular contact with children. The Protection of Children (Scotland) Act 2003 extends disqualifications which already exist in England and Wales to Scotland, except for those listed provisionally on the list kept for England and Wales under the Protection of Children Act 1999.

For further information on the DWCL see www.scotland.gov.uk/childprotection

Currently, there is no equivalent list in Scotland for those who work with vulnerable adults. Under the Protection of Vulnerable Groups (Scotland) Act 2007 the new Disqualified from Working with Vulnerable Adults List (DWVAL) will be held on behalf of the Scottish Executive Health Department and will hold a list of people who are known to be unsuitable to work in regulated adult social care positions.

The Act makes provision for the following matters concerning the protection of vulnerable groups:

- Establishing a list of individuals unsuitable to work with children and consequently repealing the 2003 Act (which established the DWCL), and establishing a separate list of individuals unsuitable to work with protected adults;
- Replacing enhanced criminal record certificates with new disclosure records for those working with vulnerable groups, whether paid or unpaid;
- Establishing a scheme for those working with vulnerable groups, membership of which enables the ongoing collection of vetting information and assessment for unsuitability to work with those groups; and
- Sharing information for child protection purposes, placing duties on relevant public bodies and organisations to disclose information when a child is at risk of harm, supported by a code of practice.

For further information on the DWVAL see:

<http://www.scottish.parliament.uk/business/bills/73-ProtVulGro/b73s2-introd-en.pdf>

6.3.4 DISCLOSURE UNDER THE FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

Section 1 of the Freedom of Information (Scotland) Act 2002 (FOISA) provides individuals with a statutory right to request information held by public authorities (including police forces). Members of the public have a right (subject to certain exemptions) to be told whether or not the police force holds the information sought and, if so, to have the information communicated to them.

6.3.5 DISCLOSURE UNDER THE DATA PROTECTION ACT 1998

Section 7 of the DPA provides 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, subject to exemptions, is the entitlement to be provided with a copy of their personal data within a statutory 40-day time limit.

The ACPO (forthcoming) Manual of Guidance on Data Protection 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 which means that forces can share information with one another. When sharing information within the service, however, it is important that there is an audit trail of the identity of the person requesting the information and of the information shared.

Some systems such as the PNC, Violent Sex Offender Register (ViSOR), and when approved, the National Firearms Licensing Management System (NFLMS), facilitate information sharing at a national level while the recent development of the Impact Nominal Index (INI) provides for the first time, an index of personal records held across the police service.

There is a clear legal distinction between making police information available within the police service and making it available to other parties. In this guidance, the police service includes forces identified in Section 1 of the Police Act 1996, the Scottish Crime and Drugs Enforcement Agency (SCDEA), 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 from agencies and people outside the police. This section focuses on information sharing with partner agencies who fall into two broad categories; those who have a statutory purpose to share or receive information and those who do not.

An example of the former is provided by Section 139 of the Behaviour Etc. (Scotland) Act 2003 which enables local authorities, registered social landlords (RSLs), the Principal Reporter and others to seek information from Chief Constables to enable them to fulfil their responsibilities under the Act. This includes disclosure and information sharing to support the creation and review of behaviour strategies under Part 1 of the Act. This also extends to the drawing up of acceptable behaviour contracts (ABCs) which, though informal, are intended to prevent any further behaviour.

Perhaps the most important recent change to the information sharing landscape has been brought about by the enactment of the Local Government in Scotland Act 2003 which placed a statutory duty on local authorities and other statutory bodies, including police forces and police authorities, to work together in order to:

- assess community needs appropriately and accurately;
- provide a basis for joint planning and targeting of resources;
- assist in performance management activities given shared targets;
- promote mutual understanding by sharing key organisational information (for example, committee decisions, resource allocations); and
- improve efficiency and reduce duplication.

Advice Note 8 in relation to this Act relates to Information Sharing and clearly states that sharing is “essential to the success of Community Planning and better joint working between agencies for the benefit of customers and citizens. ...In particular, it provides the opportunity for improved information sharing not just between public sector organisations but also with the voluntary, community and private sectors. “

It also makes specific reference to the need to share information in order to, “promote consistent and improved customer services. This might take an aggregated form (for example, general results from consultation exercises) or highly personalised (for example, individual customer records).”

For further information see <http://www.scotland.gov.uk/Publications/2004/04/19167/35264>

6.4.1 OTHER TYPES OF SHARING WHERE A STATUTORY POWER EXISTS

Before sharing information outwith the police service it must 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 children, the agency receiving the information must identify a legal power that allows them to lawfully request and process such information. Using the example given, section 56 of the Children (Scotland) Act 1995 allows the Reporter to request information from the Local Authority or police as part of an initial investigation. It should be noted that the Crime and Disorder Act 1998, in particular section 115 which gave the power to share information within Crime and Disorder Partnerships and Youth Offending Teams for crime prevention purposes is no longer relevant to Scotland.

6.5 COMMON LAW

Where the police are requested to share information with a partner in circumstances in which no statutory obligation or power exists, a lawful purpose must be established as the decision to share is risk based and must take into account the source of the information and any restrictions on its onward dissemination. This must be balanced against the requirements of the common law duty of confidence (see [Section 6.7.3](#)) and the DPA when personal information is shared. For example, a police force which plans to share information with a football club on known hooligans so that the club can ban them from attending football matches must first establish a policing purpose for doing so. In cases where, for example, the police may wish to share information about sexual offences with schools or other education establishments, the decision to share, balanced with the requirements of the relevant human rights legislation and the DPA, must be made by an officer of ACPOS rank.

6.5.1 DISSEMINATION OF INTELLIGENCE

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. Disclosure 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.

Great care should be taken prior to making a decision to disclose intelligence, not only from the perspective of considering the impact of such disclosure on any current or future investigation but also on the basis of question marks over the accuracy of any intelligence held. Where intelligence is held and is relevant, for example in respect of an individual having applied for a liquor licence, staff must in the first instance make contact with the Force Intelligence Bureau / Divisional Intelligence Manager who will determine what, if any, information can be provided to Licensing Boards and in what form.

Checklist 2: Sharing Police Information

- Where a legal gateway exists, this provides a specific purpose for sharing police information with an outside agency
- Where a legal gateway does not exist, the decision to share is based on establishing a policing purpose, or a purpose not incompatible with the purpose for which the information was originally gained, and undertaking a risk assessment.

6.6 HOW THE POLICE SHARE INFORMATION

The decision to share information requires careful judgement in which DPA and human rights conditions are balanced with policing purposes and / or the purposes of partner agencies. Any information the police are considering sharing with a partner agency must, therefore, be necessary for the purpose for which it is being shared.

The following principles help to determine whether the information the police are considering sharing is necessary and are specific to personal data only. Non-personal data, often known as anonymised or aggregated, is not subject to the same tests or considerations because an individual cannot be identified from it.

Sharing of non-personal data is widespread, for example making available information regarding housebreakings in a specific area to a Neighbourhood Watch Group, or in making available details of crime and behaviour within data-zones as part of the identification of priorities for action in either Community Plans or Behaviour Strategies.

In considering requests for police information, thought should be given as to whether it is necessary to disclose any personal information. In particular, while much may be known about an individual it will not always be necessary to disclose all of this information to satisfy the needs of the agency requesting. For instance, where sensitive medical information is known about someone suspected of behaviour, then this would not be disclosed.

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. This is a legal requirement of the DPA. Similarly 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 compliant with the principles contained within the DPA. Any conditions imposed by the originating agency should be observed before sharing takes place. Failure to do so will render the particular force and possibly the service liable to legal action and may endanger existing protocols or MOUs.

6.6.2 POLICE INFORMATION MUST BE JUDGED ON ITS OWN MERITS

The relevance of a specific record must be decided on a case by case basis. 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 SCRO. A Registered Social Landlord (RSL), requesting information regarding a tenant alleged to be regularly holding noisy parties should not be provided with conviction details in relation to street prostitution.

There may also be instances in which other information comes to light that makes the first 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 the victim.

The police may also consider it relevant, in certain circumstances, to provide a partner with information that falls outside the request. For example, information might be shared about a person who resides or associates with an individual that may help 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. In this regard, wherever possible, command and control incident summaries should not be used.

Having made a decision on whether the information is relevant for the purpose it is being shared for, the decision must be recorded so that it can be audited at a later date. Ideally this should be recorded against the record but not all systems will allow this.

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. In Scotland with the introduction of the Local Government in Scotland Act 2003, partner agencies have an overall responsibility to provide for the wellbeing of the citizens within a Local Authority area and this has generally been recognised as providing the ability to share information in order to improve public services. However, the legal obligations for processing information under common law, the DPA and human rights legislation must 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 and other individuals. Sharing personal information will be proportionate if:

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

There is a higher threshold to share personal information about less serious crimes as there is a lower public interest in this information being shared. Even greater care will require to be taken when considering whether or not to share intelligence, not only because of the possible implications for subsequent or existing police enquiries but also because of issues around the accuracy of the information.

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 and necessary to infringe any of the European Convention on Human Rights (ECHR), e.g. Article 8 ECHR Rights (Right to Privacy). It is significant that any public authority (for example, a local authority) will be bound by the same obligations under the ECHR as the police service.

6.7.2 DATA PROTECTION ACT 1998

The DPA provides a framework for decision making in respect of processing (including sharing) personal or sensitive personal data. The DPA places a requirement on chief officers as data controllers to process information in compliance with the 8 principles set out in [Section 1 - Legal Basis For Managing Police Information](#)'.

Over the years several misconceptions in relation to data protection legislation have been presented as facts. In some quarters these have become accepted as accurate interpretations of existing data protection legislation. Examples together with explanatory notes are provided within the Scottish Executive "Guidance on Disclosure and Sharing of Information" which can be viewed in full at:

<http://www.scotland.gov.uk/Publications/2004/10/20150/45696>

Further information on the DPA can be found in the ACPO (forthcoming) Manual of Guidance on Data Protection or from the Office of the Information Commissioner's website www.informationcommissioner.gov.uk

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 disclosed unless one of the exceptions to the duty applies. These are:

- Where there is a legal requirement, either under statute or a court order, to disclose the information (This includes the duty to cooperate with a local authority making enquiries under Section 21 of the Children (Scotland) Act 1995).
- Where there is an overriding duty to the public (for example, where the information concerns the commission of a criminal offence or relates to a life threatening circumstance.) Categories of public interest which might override the duty of confidence include the protection of health and morals, public safety, the prevention of crime and disorder, the protection of the rights and freedoms of others, national security and the economic wellbeing of the country. When considering disclosure under this exception consideration should be given to:
 - the proportionality of disclosure
 - the impact on or benefit to the offender
 - the impact of non-disclosure on the victim
 - supporting rights and freedoms of other individuals (e.g. intended victims) and
 - the necessity of disclosure to achieve the lawful aim
- Where the individual to whom the information relates has consented to the sharing

In certain circumstances consent does not need to be sought, such as 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.

The police also owe a duty of confidentiality to victims and witnesses of crime. A balance therefore needs to be struck between sharing such information and the rights of victims and witnesses to privacy. This is equally true in relation to the support provided by the police to victims support services. Police staff should therefore refer to relevant Standard Operating Procedures where possible to ensure compliance with legal requirements.

6.7.4 DISCLOSURE OF RESTRICTED OR CONFIDENTIAL MATERIAL TO THIRD PARTIES

In circumstances where the police, voluntarily disclose information about individuals through an ISP or statutory process to third parties, including statutory agencies when, in the usual course of events, that information would remain known only to the police (i.e. 'confidential'), then it is reasonable for the police to expect that the confidentiality of that information is respected by those third parties in the same way. In this respect the term 'confidential' is different to the meaning which it carries for the purposes of the GPMS (see [Appendix 2: Glossary for full definition](#)).

NOT PROTECTIVELY MARKED

The majority of third parties that the police share data of a personal sensitive nature with do not know or adhere to the principles of the GPMS in respect of its definition for 'RESTRICTED' and 'CONFIDENTIAL'. A different approach is required in dealing with these third parties to ensure the protection of the 'confidentiality' of the information shared. By whatever means that information is transmitted to a third party, the police have a clear assumption that the 'confidentiality' of that material will be respected by the receiver.

The individual who is the subject of such confidential information has a legitimate expectation that the police will not disclose it to any other person who is not entitled to have it. To do otherwise would leave the police service vulnerable to challenge by that individual.

Such information is certainly personal data as defined by the DPA 1998 and can also be sensitive personal data insofar as it relates to, *inter alia*, the sexual life and / or health of an individual, the allegation of the commission of offences by or against that individual, and so forth. Sensitive personal data attracts certain protections over and above those set out in the DPA governing the handling and dissemination of personal data. Disclosure of information gathered by the police to statutory third parties would not be in breach of the DPA.

There is also the matter of subsequent disclosure of such police information by one statutory agency to another in circumstances where the police force / agency from which the information originated is ignorant of that further disclosure. The recipients of such information first transmitted by the police should not assume any entitlement to further disclose or copy their contents to any other person (statutory agency or otherwise) and that to make such unauthorised further disclosure might carry serious consequences.

Apart from the provisions of the DPA, at common law the confidentiality of the material held by the police about these individuals is not absolute. Confidentiality may not be maintained in the face of any, and all, requests or orders for its eventual production against the wishes of the police service. The confidentiality of the material may, for example, be overcome where an Order of a civil Court has been made requiring production of same.

This procedure is more generally known as 'Commission and Diligence' and is within the oversight of an appointed Commissioner. There is provision within criminal proceedings for an almost identical procedure to be adopted where the parties involved will generally be the accused person and the Crown only.

In these types of circumstances legal frameworks governing such disclosures provide certain means of maintaining the confidentiality of documents, however the Court may allow the information to be seen by all parties at the decision of the relevant Commissioner or Sheriff.

It is best practice that, when an ISP is being drawn up between the relevant parties, a section is enclosed with appropriate wording, whereby if a third party is subject of such a request, that they immediately notify the originator of that information. This will give the originator, the opportunity to assess the original information and if required make their representation at the relevant stage of the process, that the material is confidential and should not be disclosed.

6.8 SHARING THROUGH AN INFORMATION SHARING PROTOCOL

Information Sharing Protocols (ISPs), should be used when there is a history of previous requests either to or by the police for information to be shared or where a new arrangement is being considered. ISPs are simply a formal arrangement between agencies who wish to share personal information and should be held and managed within the force. The IMS must clearly state where ISPs are stored, how many the force has and who has responsibility for their maintenance.

Establishing an ISP has a number of advantages. In particular they assist in:

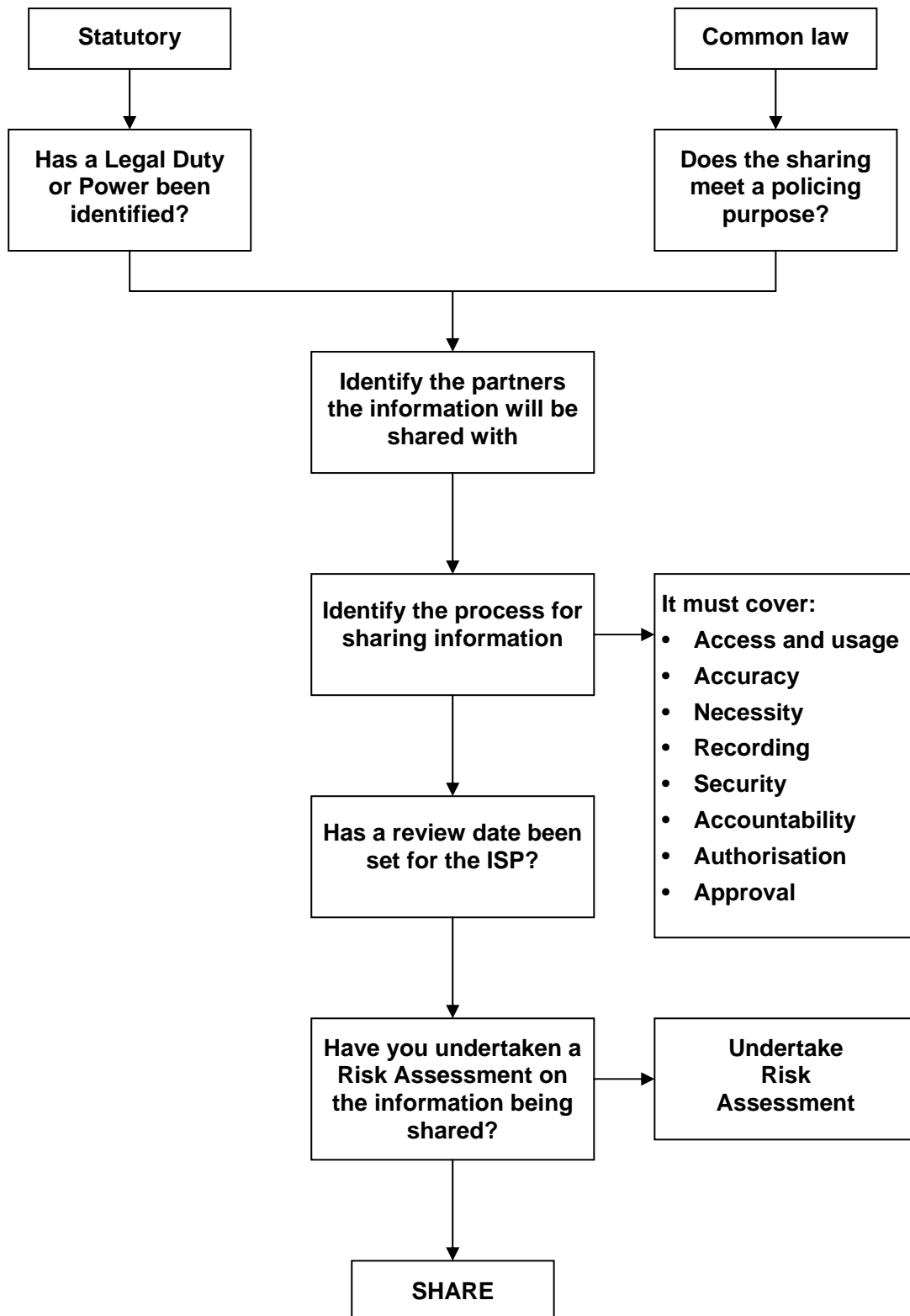
- Ensuring that information can be shared lawfully;
- Ensuring consistency in the way information is shared;
- Allowing the police to place reasonable and lawful conditions on the way information will be handled by the partner agency and vice versa; and
- Helping to build confidence in the role that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

A number of such protocols governing sharing are in place throughout Scotland covering a variety of situations e.g. Child Protection and Behaviour, which have resulted from an awareness that public bodies must work together to tackle jointly owned problems and must provide guidance to staff on the various issues around sharing such as the:

- Purposes of the protocol
- Circumstances when sharing can be carried out
- Procedures to be adopted when receiving requests
- Manner in which information is stored (especially with regard to security and auditing of sharing); and
- Key post holders with responsibilities in respect of monitoring / managing its operation.

The flowchart on the next page sets out the process of developing an ISP. Where they already exist the flowchart can be used as a 'check and balance' to ensure that existing arrangements enable consistent and lawful information sharing.

Figure 1: Information Sharing Protocol (ISP) Process Chart



6.8.1 ESTABLISHING A PURPOSE FOR THE CREATION OF AN INFORMATION SHARING PROTOCOL

All protocols must identify the reasons for sharing personal information, stating whether partners have a statutory duty to share or merely a power to share personal data. The purpose of the data sharing arrangement must be approved, understood and formally agreed by those entering into a data sharing agreement.

When first considering a data sharing initiative, organisations will have to satisfy themselves that it is lawful. For help refer to the Department for Constitutional Affairs publication "[Public Sector Data Sharing - Guide on the Law](#)" available at:

<http://www.foi.gov.uk/sharing/toolkit/infosharing.htm#part2>

This will be done by referring to the relevant legislation (sometimes referred to as the legal gateway) that is being relied upon. In addition to this, the protocol should mention that partners will have to comply with the DPA, Article 8 of the ECHR, the Freedom of Information (Scotland) Act 2002 and the common law duty of confidentiality.

Any member of police staff considering creating a protocol or who is requested to become a participant to one should in the first instance seek guidance from their force's legal services, data protection or disclosure and information security business areas as they will have had experience of the force's involvement in previous information sharing arrangements.

6.8.2 CONSENT AND THE DATA PROTECTION ACT 1998

A common approach to the issue of consent requires to be agreed. Should consent be regarded as necessary to allow collection, or disclosure of information, it has to be informed, specific and fair. The protocol should mention that when obtaining consent, the data subject must be informed of the purpose for which the information is being collected, how it will be used and with whom it will be shared. Also, it should state that if consent is sought and refused, objections must be recorded appropriately and each organisation must abide by the refusal unless legal recourse is sought.

Of course in some cases it may not be reasonably practical to obtain consent (e.g. if someone is very ill). In these instances, risk assessments and a proportionality test should be conducted between the individual's right to confidentiality, and the need for reasonable intrusion. The protocol should give brief details of how this test will be carried out.

If, as is likely to be more common, statutory powers are to be applied to allow data sharing without consent, this should still be done in accordance with the DPA. It is good practice to explain in the protocol why these powers may be applied and to notify the public and signatories of the proportionality test that will be carried out to determine whether it is reasonable to disclose personal information.

Details of the partner agencies and names, addresses and contact details must be recorded on 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 around the duty of care to persons or the furtherance of a policing purpose.

6.8.3 SETTING OUT THE PROCESS FOR SHARING INFORMATION

Setting out in the agreement the process for sharing is particularly important as it provides those involved with a clear understanding of how information will be shared, to whom and when. It also represents an opportunity for all partners to identify relevant, reasonable or lawful conditions within the protocol on how the partner agencies (or specific agency) may use the information. The following questions should be asked when developing an ISP.

What information is being shared?

The ISP will need to set out the type of information being shared. This could include details of individuals, convictions, warnings or other information. It may also be necessary to identify where the information is being held. Any information being shared must, 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 personal data that may compromise an operation or place an individual at risk of harm. The police will need to have regard to 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 in place a policy for the secure storage and processing of information. Where the police are considering sharing information with others who are not obliged to adhere to the GPMS, particular care should be taken to ensure that all parties understand the sensitivity of the information and the requirement to ensure its confidentiality, integrity and availability and that the Data Protection principles which apply to all instances of disclosure are applied rigorously.

It should be borne in mind that other agencies will have equal concerns vis-à-vis the police force's procedures in respect of all of these issues and are likely to insist that all parties to the protocol agree to uphold their responsibilities for data protection in respect of recording, storage, security, access, auditing, and of course secondary disclosure.

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.

How long will the information be retained for?

The ISP 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. Where disclosure takes place through the use of future shared software programmes, such as with the multi-agency software programmes 'e-Care' or 'Caseworks' all disclosure requests and responses will be automatically audited via the use of on screen formats. Any additional e-based arrangements should ensure that similar procedures are included as part of the business benefits of such systems.

Who is accountable for the Information Sharing Protocol?

Every individual involved in the drafting of an ISP 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 ISP within forces and partner agencies should be clearly stated on the registered file. It is important to stress however that it is the responsibility of every member of staff who processes personal data as part of the agreement to act within the law.

Who will approve and authorise the ISP?

Once the ISP has been finalised, the force / agency and partner agencies must ensure that they fully understand and agree with the purpose, process, and conditions of the agreement. Approval within a force will normally come from a business area owner but this should only be sought once all stakeholders within the force have been involved in the drafting of the ISP and all concerns have been managed. Examples of specialist stakeholders include FOI, Disclosure, DPA Officer, ICT, Legal Services, Information Security but consultation should take place widely to ensure protocols are fit for purpose. Signature to the protocol should come from a senior member of staff, typically an officer of ACPOS rank 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 processing the 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 8 principles of the DPA:

The First Principle:

'Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'

The Second Principle:

'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'

The Third Principle:

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'

The Fourth Principle:

'Personal data shall be accurate and, where necessary, kept up to date.'

The Fifth Principle:

'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

The Sixth Principle:

'Personal data shall be processed in accordance with the rights of data subjects'

The Seventh Principle:

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

The Eighth Principle:

'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.'

Where will the ISP be held?

All ISPs must be held centrally and made freely available to staff. A high level summary of the agreement can be added that provides a brief description of the purpose, partners and processes, (including subject access rights) together with the name of the individual who is tasked with maintaining the agreement. Where possible, ISPs should be made publicly available as the process for sharing should be seen to be as open and transparent as possible.

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 INFORMATION SHARING PROTOCOL

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

Equally, however, care should be taken to ensure that where possible, requests for information are, with the exception of emergency requests, not provided verbally. In the case of oral disclosures and exchanges, a contemporaneous note must be made by any member of a partner agency's staff who has either given or received information. The note made must contain details of the information given or received, the purpose for which it was given or received, the name and designation of the person to whom the information was given or from whom it was received, and the time, date and place at which the information was given or received. Where personal information is disclosed during a pre-planned multi-agency meeting the minutes should clearly record this (though obviously not the personal data).

Any decision not to disclose information must also be recorded, together with the reasons for the decision. In the case of police officers, such notes must be made in their official notebooks or on an appropriate software programme where it allows this. Members of staff of all other partner agencies should be requested to make file entry notes, which must thereafter be preserved.

6.9 REVIEW

An essential part of any ISP is the ability to review. The aim of the review is to ensure that the agreement is achieving its purpose and the actual process of sharing is operating smoothly, according to the procedures set out, and, very importantly, within the law. It should be carried out in conjunction with partner agencies and be performed on an annual basis, except where the agreement is in its first year where it should be reviewed after the first 6 months.

The following stages set out the process of review.

6.9.1 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 remain relevant. Some protocols 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 protocol 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. A review may identify the 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, if there are substantial amendments to the original ISP, a new ISP may be necessary.

6.9.2 DOES THE INFORMATION SHARING PROTOCOL HAVE THE CORRECT 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 protocol accordingly.

6.9.3 HAS THE REVIEW IDENTIFIED ANY EMERGING ISSUES?

Reviewing the protocol provides an opportunity to discuss any problems that may have arisen during the period of the 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 indeed, any new legislation enacted that may have an impact on the agreement. Again, any changes will need to be recorded, approved and added in any addendum.

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

At the end of the review, a decision should be taken on whether to extend the lifetime of the protocol (typically for one year) or whether to terminate it. Any decision should be recorded with the reasons for choosing a particular course of action. Where it is decided to revoke an ISP this should be communicated to all relevant personnel who have previously been using the protocol to share information.

6.10 THE PROCESS OF SHARING POLICE INFORMATION OUTWITH THE TERMS OF AN INFORMATION SHARING PROTOCOL

Where an ISP does not exist, or the decision to share is a one-off, [Checklist 3](#) overleaf provides a reminder to staff of the key questions that will help to ensure any information sharing is done lawfully.

Checklist 3: Sharing Police Information Outside an ISP

- Who is asking for the information?
- Have you recorded their name, position, organisation and contact details?
- Have you verified the identity of the person making the request?
- What information is being asked for? What purpose will it be used for?
- Is the information being requested personal data?
- Has a legal gateway or a policing / lawful purpose to share information been established?
- If yes, how do they wish the information? Ensure that the process for sharing the information is secure and managed effectively.
- When do they want the information?
- Do you require to clarify the legitimacy of the request / information to be provided with supervisors or seek advice on the law?
- Record your decision, how you made it and what information was shared.

6.11 RESPONSIBILITIES FOR MANAGING INFORMATION SHARING

The guidance sets out the responsibilities of managers, supervisors and users in this section as follows:

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 ISPs are held and managed centrally within force / agency.
- Ensuring that the process of sharing information is adhered to by both those in a supervisory and user capacity.
- Authorising ISPs.
- Ensuring that staff who have a responsibility for sharing information are appropriately trained.

6.11.2 SUPERVISORS

- Supporting staff to share information appropriately.
- Auditing, by means of dip sampling, 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 ISPs are reviewed in accordance with force / agency 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 DPA 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 a risk assessment where the sharing is carried out with partners not required to adopt GPMS or who do not have a statutory purpose to share information.
- Recording any decision to share in accordance with the ISP. Similarly, users are responsible for recording any decision not to share information on the relevant system.

NOT PROTECTIVELY MARKED

- Ensuring that the information being shared meets a policing purpose or can be lawfully disclosed for a statutory purpose and is proportionate and necessary.
- Following existing force / agency policies set out in the IMS that comply with this guidance.

Section 7

RETENTION, REVIEW AND DISPOSAL

This section explains what is meant by the terms retention, review and disposal. It provides guidance on the timeframes for retaining and reviewing information and the criteria to use for deciding whether to retain or dispose of information. This section should be read in conjunction with the associated document - ACPOS Records Retention Schedule

Key principles of this section are:

- Records must be managed properly and consistently in order to ensure that they are adequate, up to date and remain necessary for a policing purpose.
- The type and amount of information held on an individual or a subject must be proportionate to the risk they pose to the community.
- The retention, review and disposal policy, procedure and process should be documented and available for audit purposes.
- Review of information is central to risk-based decision making and public protection.
- Records should be disposed of when there is no longer a legislative, statutory or policing purpose for retaining them and they hold no historical value for future research.
- Records will be managed in accordance with ISO 15489. (See Appendix 2: Glossary)

7.1 LEGAL ISSUES

There are a number of specific legal provisions that are relevant to the retention, review and disposal of police information, summarised below. All documents whether electronic or hardcopy will require to be marked with the appropriate GPMS marking.

Refer to the *ACPOS Records Retention Schedule* for full details.

7.1.1 HUMAN RIGHTS ACT 1998

Public authorities, including police forces / agencies, must act in a way that is compatible with the ECHR. In relation to record retention this requires a proportionate approach to the personal information held about individuals. The decision to retain personal records must 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 must be met in order to retain records about relatively minor offending.

Recent 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.

7.1.2 DATA PROTECTION ACT 1998

The police service can lawfully hold records of personal information provided that they comply with the DPA. Other legal requirements governing the holding of personal information should be considered in conjunction with the DPA.

For further information see [Section 1 The Purpose of Managing Police Information](#).

7.1.3 FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

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

The FOI(S)A makes it an offence to deliberately alter, erase or destroy records once an application for access to them has been made in an effort to avoid having to disclose them. This means that forces / agencies may have to disclose any records that they hold, even if these records are inaccurate, excessive or otherwise contravene the DPA. It is, therefore, imperative that all records are properly reviewed so that they can confidently be disclosed if required.

7.2 RETENTION

All police information and records are subject to agreed standard retention periods as defined in the [ACPOS Record Retention Schedule](#). This national agreement assists forces and agencies to comply with legislative obligations and supports good business practice while providing information sources required for policing purposes. Accompanying the [ACPOS Records Retention Schedule](#) is the [ACPOS Retention Crime Policy Guidelines](#) document. This permits flexibility when assessing particular records in relation to the threat and risk posed from their destruction within the timeframes set in the Schedule. Forces / agencies may decide to retain information for longer periods than those prescribed if it is justifiable, proportionate and necessary.

Retention periods wherever possible are based on a wide range of applicable legislation. However the majority of information collected for a policing purpose is not subject to direct legislative statements regarding the length of retention. Therefore retention is pre-planned to meet the policing purpose, but permits specific changes where circumstances require it.

The length of retention is based on the use and value of the information as defined by police practitioners.

Complying with the retention periods in the [ACPOS Records Retention Schedule](#) supports:

- the sharing of information between authorised parties; and
- standardised applications provided to support the policing purpose and is reliant on common data standards for the creation, capture, recording, management and disposal of information.

Information retained must be:

- managed in accordance with security policies and GPMS.
- processed, stored, copied, shared, and disposed of in a manner which does not compromise the confidentiality, integrity, and availability of the information and is commensurate with its protective marking.
- searchable and retrievable by all staff who are appropriately vetted and have a need to know.
- subject to audit regardless of whether the information is retained in an electronic or hard copy format. The minimum requirements for audit are as follows:
 - Electronic - Identity of user; log on / off information including time, date and location; Failed log on / off information including time, date and location; Actions taken while logged on including data viewed, data amended, data printed, data transmitted or transferred (including copy/paste); Actions failed while logged on (system access denied); data subject of search while logged on (data not held but still searched).
 - Hard copy - Identify the individual accessing the information; actions undertaken including removal, copying, amendment, sharing, and destruction.

Retention of information relating to criminal activity and known and suspected offenders allows the police service to develop and use a variety of policing tactics. It is however impractical, unlawful and in some instances unhelpful for forces and agencies to retain every piece of information collected indefinitely. Pre-defined retention periods provide the basis for information management. Once set, the practical implications of retention must be considered and determined by forces and agencies. In some circumstances where individual parts of records cannot be separated, for example in police notebooks, the record should be retained in its entirety.

7.2.1 DUPLICATION

Retention recommendations are for original or master sets of records. Duplicate records can be destroyed at any point appropriate to the work of the organisation and when the purpose for which they were created has been fulfilled. Duplication across systems can pose a risk, as does all information held in dispersed silos. Consideration should be given to the amount and type of detail on systems and the extent of duplication. Where manual records have been destroyed after being copied to electronic systems, they should meet the standards included in BSI DISC PD0008. It may be more practical to retain electronic rather than paper records and provided the information is accurate, searchable and maintains its integrity, the manual records can be destroyed. It is particularly important that records created electronically stay on that format as they can then maintain and demonstrate the relationship with electronic information sources.

7.2.2 PRODUCTIONS

Productions, and in particular documentary productions are subject to separate rules and procedures and staff must refer to force / agency procedures and policies for direction on the management of such items. For further information refer to *ACPOS Records Retention Schedule*.

7.2.3 STORAGE AND PRESERVATION

Forces and agencies should develop and implement a comprehensive and manageable storage and preservation strategy to address lifetime management considerations, including:

- The format that information is stored on, both manual and electronic.
- Migration of information to new applications and operating systems.
- Preservation of information, particularly long term retention of electronic records to guarantee its content, context, structure and integrity.
- Audit and compliance checks to demonstrate transparency of use and management.
- The impact and benefits of use of near-line and off-line storage to promote systems efficiency.
- Ensuring that the security requirements for the information are defined and implemented.
- An audit to ensure that information remains complete, accessible and has not degraded.

7.3 WHY REVIEW POLICE INFORMATION ?

In certain instances the [ACPOS Record Retention Schedule](#) requires information to be reviewed to consider whether it should continue to be retained or should be destroyed. Scheduled reviews occur when the nature and context of the information or record series do not allow definitive pre-defined scheduling of retention and destruction and instead are marked as 'review' in the [ACPOS Record Retention Schedule](#).

Review procedures must be as practical and non-bureaucratic as possible. Those staff undertaking reviews must consider the risk and be able to identify information valuable for policing purposes. Review procedures will help to ensure that information retained is lawfully held and will help prevent forces / agencies being overloaded by the volume of information captured and recorded. Reviewing information held by forces / agencies to determine its adequacy and continuing necessity for a policing purpose is a reliable means of meeting the requirements of the DPA.

In reviewing information, certain considerations must be addressed, however different types of information may require different review procedures. Review of person records, for example, may use criteria that varies from that used for general subject records. Some criteria are standard for all records:

- Is there a continuing policing purpose to hold the information?
- Is the information adequate, up to date and not excessive?
- Are the records compliant with relevant legislation?

Information may be retained and reviewed without breaching principle 5 of the DPA as long as an ongoing policing purpose can be defined and demonstrated. For that reason and also to inform other users, it is important to record the outcome of a review of records, irrespective of whether the decision taken is to retain for a further period or to destroy.

Intelligence reviews will be subject of their own robust reviewing process.

7.4 HISTORICAL DATA

Certain specific records may be of historical value and where this is recognised they should be appropriately designated and transferred to an archive either within the force / agency or subject to a legal agreement with a local government archives office. These records are outwith the operational environment and it must be made clear in the IMS that they are retained for historical purposes only. The [ACPOS Record Retention Schedule](#) specifies those records that are considered to be of historical value.

7.5 DISPOSAL

The collective range of processes associated with records retention, destruction or transfer is known as disposal or disposition. Destruction of records, irrespective of format is the process of eliminating or deleting records beyond any possible recognition.

7.5.1 RECORDING DISPOSAL

On completion of the retention period or a review leading to a decision not to retain, the record must be destroyed following secure disposal methods in accordance with the requirements of the GPMS. A record of information destroyed, at record series level must be retained as required by the section 61 Code of Practice under the FOI(S)A 2002.

The IMS will specify a destruction process that includes the date of the decision, description (which may include the number and type of records and / or file title, series description, volume etc.) and reason for disposal.

7.5.2 METHOD FOR DISPOSAL

The method of disposal for records of police information will depend on the GPMS protective marking. The *Cabinet Office (n.d) Government Manual of Protective Security* and the *ACPO / ACPOS Handling of Protectively Marked Material*, specify requirements for the handling and disposal of classified material. All forces / agencies must develop and implement a policy for disposing of records in accordance with these schemes.

7.6 AUDIT OF RETENTION, REVIEW AND DISPOSAL

The IMS will specify an audit schedule and process to monitor that retention, review and disposal is being carried out in accordance with this manual. The IMS should also identify who is responsible for the completion of the audits. It will include;

- Date of decision.
- Number of records.

Under no circumstances should records documenting a decision to dispose of information hold the personal details of individuals referred to. As in [Section 7.5.1: Recording Disposal](#), a record of information destroyed shall be retained at record series level in the records. The review process outlined in this guidance will ensure that forces / agencies 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 / agency should have any indication they ever had it. The exception to this rule will be in respect of documents marked as SECRET or TOP SECRET, which will comply with the GPMS destruction policy whereby the audit log will identify the nominal that records have been destroyed.

For further information see [ACPOS Records Retention Schedule](#).

7.7 RESPONSIBILITIES

The guidance sets out the responsibilities of system owners, managers, supervisors and users in this section as follows:

7.7.1 SYSTEM OWNERS

- 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.

7.7.2 MANAGERS

- Ensure a dip sample of records held by their department is undertaken.
- Ensure staff responsible for undertaking reviews are trained appropriately.

7.7.3 SUPERVISORS

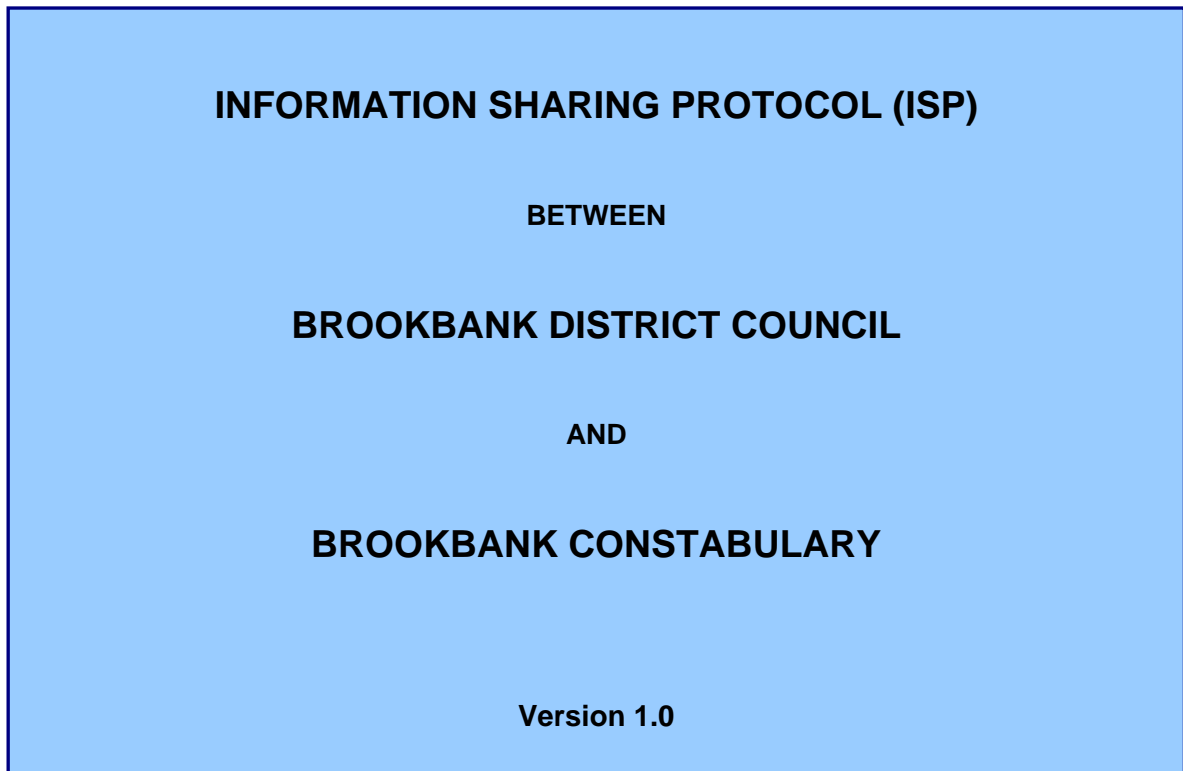
- Authorise the outcome of all reviews conducted in their area of responsibility.
- Ensure that the review policy in the IMS is followed.
- Provide feedback to staff.
- Ensure users of systems are aware of and adhere to force / agency policies and procedures relating to information management and systems.

7.7.4 USERS

- Follow this guidance for reviewing records.
- Access, understand and follow force / agency security policies and operating procedures.
- Establish and enter the review date for a record at the point of creation.
- Ensure that information to be disposed of is not duplicated and, therefore, retained elsewhere.

NOT PROTECTIVELY MARKED

Appendix 1 -ISP Template / Example



SUMMARY SHEET	68
1. Introduction.....	69
2. Purpose	69
3. Partner(S).....	69
4. Power(S)	69
5. Process	70
6. Signature	73
Form: Request for Personal Information	74

SUMMARY SHEET

Title of ISP

ISP Ref:	WC001/BrookbankDC
-----------------	-------------------

PURPOSE	To take action against crime and antisocial behaviour in properties owned and managed by Brookbank District Council.
----------------	--

PARTNERS	Brookbank Constabulary Brookbank District Council
-----------------	--

Date Agreement comes into force:	01/01/06
---	----------

Date of Agreement Review:	01/07/06
----------------------------------	----------

Agreement Owner:	Brookbank Constabulary
-------------------------	------------------------

Agreement drawn up by:	Inspector Bob Jones
-------------------------------	---------------------

Location of Agreement in force:	S:/Information Sharing/Housing/Brookbank
--	--

Protective Marking:	NOT PROTECTIVELY MARKED
----------------------------	-------------------------

VERSION RECORD

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

1. INTRODUCTION

- 1.1 Brookbank Constabulary are committed to partnership working and continually look for opportunities to work more closely with local authorities and other partner organisations to detect, prevent and reduce crime and antisocial behaviour.
- 1.2 This agreement outlines the need for the police and involved partners to work together to alleviate crime and 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 behaviour in properties owned and managed by Brookbank District Council. It will incorporate measures aimed at:
- Facilitating a coordinated approach that targets crime and antisocial behaviour;
 - Facilitating the collection and exchange of relevant information;
 - The pursuit of civil or criminal proceedings - either by Brookbank Constabulary or Brookbank 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 Brookbank Constabulary and Brookbank District Council to combat crime and antisocial behaviour.

3. PARTNER(S)

- 3.1 This agreement is between the following partners:
- BROOKBANK DISTRICT COUNCIL of 2-5 Ford Lane, Brookbank, Brookbank
BROOKBANK CONSTABULARY of County House, Brookbank

4. POWER(S)

- 4.1 This agreement fulfils the requirements of the following:
- Behaviour etc (Scotland) Act 2004, section 139;
 - The Housing (Scotland) Act 2001;
 - The Local Government in Scotland Act 2003, sections 20 & 23;
 - Common Law Powers of Disclosure;
 - The Rehabilitation of Offenders Act 1974;
 - The Human Rights Act 1998 (article 8); and
 - The Data Protection Act 1998 (sections 29(3) & 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 must be justified on the merits of each case.

5.2 TYPES OF INFORMATION TO BE SHARED

Brookbank Constabulary will share:

- De-personalised information relating to crime or behaviour in the areas of housing owned or managed by Brookbank.
- Evidence relating to a conviction of a tenant for an arrestable 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.
- An admission of behaviour by the tenant, member of the resident family or invited visitor, evidenced by a pocket note book signature by the offender.
- Evidence from police records of incidents of 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 statement maker for that statement to be disclosed for use in civil proceedings.

Brookbank District Council will share:

- Evidence, including complaints from neighbours or the public relating to criminal or 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 must not be disclosed to any third party without the written consent of the agency that provided the information. It must 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 must appoint a single point of contact (SPoC) who must work together to jointly solve problems relating to social tenants. The sharing of information must only take place where it is valid and legally justified.

- 5.4.2 SPoCs must meet regularly to discuss and prioritise incidents of criminal or 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 must 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 must meet one or more of the policing purposes.
- 5.4.4 Within Brookbank Constabulary, the file must be held and managed centrally by a force / agency Information Manager. This arrangement must be replicated within Brookbank District Council.
- 5.4.5 The designated police officer must 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 'CONFIDENTIAL - Request for Personal Information' Form.
- 5.5.2 Requests may be made by fax but care must be taken where personal information is shared. Similarly, requests and replies should not be communicated via e-mail as the Internet is not secure for the transmission 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 Brookbank District Council Prior to Conviction:**
- 5.5.6 In some cases, civil proceedings may be a more appropriate route to take than a criminal prosecution. 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 when a criminal investigation has already started, any decision on whether or not to proceed with a criminal prosecution must be referred to the designated police officer who will liaise with COPFS. 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 COPFS. The police cannot provide opinion evidence.

5.5.9 Where a complaint of 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 Brookbank District Council must write to Brookbank Constabulary informing them that action is being considered. The tenants 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; or
- Persons arrested.

5.5.11 Officers attending incidents should make detailed notebook 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:**

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 **RETENTION, REVIEW & DELETION**

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 delete it when it is no longer required. The force / agency may also want 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 / agency 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 ISP will be reviewed six months after its implementation and annually thereafter. The nominated holder of this agreement is Brookbank Constabulary. It is based on the national template for Information Sharing which forms part of the guidance issued on the Management of Police Information by ACPOS and the Home Office.

5.8 **INDEMNITY**

5.8.1 Brookbank District Council as receivers of police information will accept total liability for a breach of this Information Sharing Protocol (ISP) should legal proceedings be initiated 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 is 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 Brookbank Constabulary:

Title:.....

Rank/ Position:.....

Date:.....

Signed on behalf of Brookbank District Council:

Title:.....

Rank/ Position:.....

Date:.....

NOT PROTECTIVELY MARKED
RESTRICTED (When Complete)

Form: Request for Personal Information

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	
Post Code	
Previous Address	
Post Code	

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)

Note: The default GPMS marking for this form is RESTRICTED once completed, whoever the GPMS marking must reflect the content of the request for information being made. If a higher GPMS marking is required then the requester must change the marking as appropriate.

Appendix 2

GLOSSARY

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

Area Command / Division

A geographical area within a police force / agency also known as an area, division or command unit.

BS DISC PD0008

The Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.

Business area

A business area where police information is recorded for a specific policing purpose as defined in section 1, i.e.:

- Crime
- Intelligence
- Domestic Violence
- Child Abuse Investigations
- Firearms Revocations and Refusals
- Custody

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 include the following highlighted areas which are particularly pertinent to the police;

- 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.

Further information can be found in the [*ACPO/ACPOS Guide to Handling of Protectively Marked Material*](#).

Confidential information

Confidential information is defined in the statutory Covert Surveillance Code of Practice made under RIPA and RIP(S)A 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 / agency or area command / division.

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 series

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

Criminal History System (CHS)

Maintained by the Scottish Criminal Records Office (SCRO)

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 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.'

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 / agency 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.

Disclosure Scotland

The central registered body in Scotland for disclosure under Part V of the Police Act 1997.

Disposal

The deletion or destruction of information from all police systems, justified through the evaluation and review process, to the extent that it cannot be recovered.

ECHR

European Convention on Human Rights

EEA

European Economic Area

Enforcement notice

The Scottish 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 Act. 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 on a point of law may be made to the Court of Session which may confirm, amend or overturn the notice. In the absence of an appeal, however, if the authority fails to comply with an enforcement notice then the Scottish Information Commissioner may apply to the Court of Session which will deal with the matter as a contempt of court. The Scottish Information Commissioner may serve an enforcement notice upon a data controller who has contravened or is contravening any of the Data Protection principles.

EU

European Union member countries.

FOI(S)A

Freedom of Information (Scotland) Act 2002.

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 and RESTRICTED. All protectively marked assets should be physically labelled. For further information see [Manual of Protective Security](#) or the [ACPO / ACPOS Guide to Handling Protectively Marked Material...](#)

Handling Codes

Handling codes allow the straightforward reporting of decisions on the suitability or otherwise of exposing certain information to other parties.

IMPACT

Intelligence Management, Prioritisation, Analysis, Coordination and Tasking – programme to deliver a national IT intelligence system.

INI

IMPACT Nominal Index.

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 / agency to another or to any non-police organisation or person.

Information Sharing Protocol (ISP)

An ISP is a legal agreement between organisations who wish to share personal information with each other.

Intelligence

Intelligence in this guidance is information that is subject to a defined evaluation and risk assessment process in order to assist with police decision making, see [Section 4: Recording of Police Information](#).

Intelligence Products

Intelligence products are the information sources that drive the Tasking and Coordination 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, front line officers and support staff as to what information and intelligence 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 Source Register (ISR)

The ISR for the recording of details around sources of intelligence.

Intelligence system

An intelligence system refers to the holding of information which has been evaluated to have an intelligence value.

ISO 15489 -1

Provides guidance on managing records of originating organisations. All of the elements are recommended to ensure that adequate records are created, captured and managed.

- applies to records in all formats and media, created or received by an organisation in the conduct of its activities,
- provides guidance on determining the responsibilities of organisations for records and records polices, procedures, systems and processes,
- provides guidance on records management in support of a quality process framework
- provides guidance on the design and implementation of a records system

ISO 15489 -2 is the implementation guide to part 1

Law Enforcement Agency (LEA)

For the purpose of this guidance it is an agency with whom the police have an agreement to pass intelligence records to, for example, HMRC.

MAPPA

Multi-Agency Public Protection Arrangements.

Metadata Standards

Taken from BS ISO 15489. Data describing context, content and structure of records and their management through time.

MO

Modus Operandi.

NFLMS

National Firearms Licence Management System.

National Information / Intelligence Report (5x5x5)

The National Information / Intelligence Report is the national report for recording information for potential inclusion into 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-led principles within law enforcement, see [ACPOS \(2006\) *Guidance on the National Intelligence Model*](#).

National Strategic Assessment

An ACPO document that evaluates strategic issues facing the police service annually.

Near-line

Records that are held between a live system and off-line system, but which are more easily accessible, for example a mirror system or archived dataset that you have to select to search for example.

Nominal Record

For the purpose of this guidance a nominal record refers to a record containing the minimum of a person's forename, and family name, partial name, and any nickname or aliases and where relevant date of birth.

Off-line

Records that are not held on a live system and are therefore not immediately accessible, for example on a CD-ROM, back-up tape or off-line server.

PNC

Police National Computer.

Personal data

Defined in the DPA as data relating to an identified or living individual.

Police purposes

This guidance adopts the definition of policing purposes as outlined in this document; i.e. protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; any duty arising from statute or common law.

Police Service

For the purposes of this guidance police service includes SCDEA and all Home Office and non-Home Office police forces.

Police Staff

Police Officers, force Support Officers, Cadets, Traffic Wardens, Special Constables, Community Support Officers and any other person, whether seconded or temporarily under the control or direction of the Chief Constable (e.g. agency staff).

Potentially dangerous person

An individual who, although never convicted, has come to the attention of police through behaviour which suggests that they have the capacity to cause serious harm.

Problem profile

A 'problem profile' is an assessment of a specific problem or series of problems, including criminal activities, threats to public safety and antisocial 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, COPFS.

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 (Scotland) Act 2002.

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.

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 captured, for example, in the case of an intelligence system, information will be recorded on a National Information / Intelligence Report (5x5x5).

RESTRICTED

In line with the GPMS, accidental or deliberate compromise of assets marked as 'RESTRICTED' would be likely to:

- Cause substantial distress to individuals;
- Prejudice the investigation or facilitate the commission of crime;
- Breach proper undertakings to maintain the confidence of material provided by third parties;
- Breach statutory restrictions on disclosure of material;
- Disadvantage the police service in commercial or policy negotiations with others; or
- Undermine the proper management of the public sector and its operations.

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 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 are compliant with the eight principles of the DPA.

Sanitised Intelligence

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.

Scottish Intelligence Database (SID)

National Intelligence Database for Scotland hosted by SCRO.

SCRO

Scottish Criminal Record Office responsible for the maintenance of the Scottish Criminal History System (CHS).

SCRS

Scottish Crime Recording Standard.

Sensitive Personal Data

The DPA 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.

Serious Organised Crime Agency (SOCA)

The agency responsible for the management of level three serious organised criminality in the UK.

Serious Crime Enquiries

In general terms the expression serious crime enquiry means criminal investigations into exceptional cases. It is applied to crimes involving acts or attempts of:

- Murder, Culpable Homicide (including statutory) & Drug Related Deaths
- Serious & Series Sexual Offences
- Serious Violence
- Abduction involving Extortion
- Terrorism
- High Value Acquisitive Crime
- Major Drug Trafficking

Sexual or violent offender

Section 327 of the Criminal Justice Act 2003 defines a sexual or violent offender.

Strategic Assessment

Strategic Assessments are the key intelligence products that inform the Strategic Tasking and Coordination 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, consider current activities as well as try to provide a forecast of likely developments. This document is produced at a national (UK), Scottish, force and divisional (depending on force) level.

Identifies medium and long term policing issues to determine resource, funding and communication requirements.

Subject access

This is the term given to the right of any individual within the DPA 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.

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.

URN

Unique Reference Number

ViSOR

Violent 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 and a police service nationally agreed vetting policy.

Vulnerable adult

In the context of this guidance, the following definition of 'vulnerable adult' is: '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 3

REFERENCES

NOT PROTECTIVELY MARKED

ACPO (2004) *Code of Practice on Data Protection*

ACPOS (2005) *Freedom of Information Manual of Guidance*

ACPO (2004) *Guidance on Investigating Domestic Violence*, Wyboston: NCPE.

ACPO (2005) *Code of Practice on the Management of Police Information*, Wyboston: NCPE.

ACPO (2005) *Code of Practice on the Police National Computer*

ACPO (2005) *Guidance on Investigating Child Abuse and Safeguarding Children*, Wyboston: NCPE.

ACPO (2005) *Guidance on The Management, Recording and Investigation of Missing Persons*, Wyboston: NCPE.

ACPO (2005) *Guidance on The National Intelligence Model*, Wyboston: NCPE.

ACPO (2005) *Practice Advice on Core Investigative Doctrine*

ACPO (2006) *Guidance on The National Briefing Model*, Wyboston: NCPE.

ACPO (2006) *Threshold Standards for The Management of Police Information*, Wyboston: NCPE.

ACPO (forthcoming) *Guidance on Public Protection*

ACPO (forthcoming) *Manual of Guidance on Data Protection*

ACPO and HMCE (1999) *Code of Practice on the Recording and Dissemination of Intelligence Material*

ACPO and HMCE (1999) *Manual of Standards for the Recording and Dissemination of Intelligence Material*

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*, version 3 2006

ACPO and HMCE (2004) *Manual of Standards for Covert Human Intelligence Sources*

ACPO and HMCE (2004) *National Standards in Covert Investigations Manual of Standards for Surveillance of Investigatory Powers Act 2000*.

ACPOS SID Rules, Conventions and Data Standards v.6 (2006)

ACPOS Manual of Guidance on the National Intelligence Model (2006)

ACPOS Records Retention Schedule

CABINET OFFICE (n.d) *HMG Manual of Protective Security*, London: Cabinet Office

Criminal Records Bureau (2006) *Criminal Records Bureau* (CRB) [Internet]. London: CRB. Available from <http://www.disclosure.gov.uk> [Accessed 6 January 2006].
Department for Constitutional Affairs (2006) *Department for Constitutional Affairs* (DCA) [Internet]. London: DCA. Available from <http://www.dca.gov.uk> [Accessed 4 January 2006].

Department of Health (2006) *Department of Health* (DH) [Internet]. London: DH. Available from <http://www.dh.gov.uk> [Accessed 24 January 2006]

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.

GREAT BRITAIN. Parliament (1956) *Sexual Offences Act 1956*. London: HMSO.

GREAT BRITAIN. Parliament (1989) *Children Act 1989*. London: TSO.

GREAT BRITAIN. Parliament (1996) *Criminal Procedure and Investigations Act 1996*. London: TSO.

GREAT BRITAIN. Parliament (1996) *Police Act 1996*. London: TSO.

GREAT BRITAIN. Parliament (1997) *Police Act 1997*. London: TSO.

GREAT BRITAIN. Parliament (1998) *Crime and Disorder Act 1998*. London: TSO.

GREAT BRITAIN. Parliament (1998) *Data Protection Act 1998*. London: TSO.

GREAT BRITAIN. Parliament (1998) *Human Rights Act 1998*. London: TSO.

GREAT BRITAIN. Parliament (2000) *Freedom of Information (Scotland) Act 2002*. London: TSO.

GREAT BRITAIN. Parliament (2000) *Regulation of Investigatory Powers Act 2000* (RIPA). London: TSO.

GREAT BRITAIN. Parliament (2003) *Criminal Justice Act 2003*. London: TSO.

GREAT BRITAIN. Parliament (2003) *Sexual Offences Act 2003*. London: TSO.

HM Government: Information Sharing Vision Statement (2006)

HOME OFFICE (2005) *PNC Code of Practice* London: Home Office

LORD CHANCELLOR (2002) *Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000*.

PITO (2005) *PNC User Manual Volumes 1 and 2*

Readhead, I (2005) ACPO Letter [Intranet] Bramshill: Centrex Available for <http://>

Scottish Parliament (2002) *Freedom of Information (Scotland) Act 2002* (FOI(S)A).

Scottish Parliament (2000) *Regulation of Investigatory Powers (Scotland) Act 2000* (RIP(S)A).

NOT PROTECTIVELY MARKED

Teachernet (2006) *Teachernet* [Internet]. London: DfES. Available from <http://www.teachernet.gov.uk> [Accessed 24 January 2006]