



**Kent
Police**

NOT PROTECTIVELY MARKED

Kent Police

Information Management Strategy, Standards and Operating Procedures

This strategy document encapsulates and underpins the Force policies/protocols inherent in managing information and provides the over-arching framework within which to implement those policies and protocols. Implicit is the understanding that policies, procedures and processes for all key elements of information management exist and that each has an owner and reference number, together with a review schedule. The key elements include vetting, information security, systems security, risk management, records management, review, retention & disposal, disclosure, dissemination & sharing and audit & quality assurance.

The existing legal framework for the management of information relating to data protection, human rights and freedom of information is acknowledged. References to the management of police information include the processes of obtaining, classifying, recording, storing, reviewing, retaining, deleting and sharing information, including personal information, for police purposes in accordance with principles governing those processes.

Strategy Reference:	
Strategy Owner:	
Contact Point:	Review Date:

Signed on behalf of Kent Police:

.....

Title:

Position:
.....

Date:

Contents

Part 1: Information Management Strategy

1. Introduction

2. Strategic Aim – Information Management

3. Information Management Values

3.1 The Standards

3.2 Business Management

3.3 People Management

3.4 Information Sharing

3.5 Data/Information Management

4. Scope of Strategy

5. Governance

6. Responsibilities

7. Relationship with Existing Policies

8. Relationship with Future Policies

9. Equality Impact Assessment

Kent Police

Part 1

Information Management Strategy

1. Introduction

- 1.1 The Chief Constable (or an officer of ACPO rank or equivalent under his direction) will establish and maintain an Information Management Strategy (IMS) within the Force, in accordance with the Management of Police Information (MoPI) Statutory Code of Practice (COP). The IMS is to take due regard of the guidance and standards to be issued under the MoPI COP except where that guidance is superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996.
- 1.2 The Force provided a MoPI implementation project team to:
- interpret the code and guidance;
 - act as the main point of contact in consultation with other national teams;
 - refine and deliver the Force MoPI implementation strategy;
 - lead on the development of information management policies;
 - work with business process owners and system owners to identify the need for changes in information systems and processes;
 - escalate items for decision to the management boards;
 - monitor progress;
 - and hand-over on-going responsibility to the key designated post holders;
 - complete the above by the 31st December 2010 in accordance with the national Force Action Plan).

- 1.3 Kent Police has a duty to obtain and use a wide variety of information (including personal information), in order to discharge its responsibilities effectively. This information management strategy (IMS) and accompanying standards, in conjunction with all other information management related policies, procedures and processes, provides a mandate for the performance of all information management functions to ensure all staff including agents, contractors and partners involved with police information, competently and efficiently carry out their duties. Within MoPI CoP a policing purpose is defined as:
- Protecting life and property;
 - Preserving order;
 - Preventing the commission of offences;
 - Bringing offenders to justice;
 - Any duty or responsibility of the police arising from common or statute law.
- 1.4 Implementation will focus on the following:
- Citizen-focused Service Delivery;
 - Governance;
 - Effective and Lawful Use of Information;
 - Information as a Force Asset;
 - Information as a Shared Resource;
 - Infrastructure and Strategic Management of Information.
- 1.5 Implementation of the strategy will incorporate ISS4PS Information System strategy for the Police Service, which will assist the Force in achieving effective police information management.
- 1.6 This IMS is not a stand-alone document. It is intrinsic to how the Force manages all of its police information within the policing context and as such informs and is informed by, all other Force policies. By its very nature, the management of all police information will form part of Kent Police usual operational business; be integrated and consistent across all business areas within the Force; and be reviewed and updated in line with other Force policies.
- 1.7 This strategy does not take a systems approach but will ensure that information is managed across all Force objectives, functions and processes in accordance with MoPI CoP.

2. Strategic Aim – Information Management

Kent Police aim to:

Provide the best possible service to our communities by providing reliable information at the point of need, where individuals understand the importance of using it correctly, sharing it lawfully and protecting it from improper use.

To achieve its aim, the Force will:

- Work to meet the required standards to comply with legislation, MoPI CoP & Guidance and relevant Force policies;
- Manage its information corporately;
- Identify and support effective practice in the management of police information across all business areas;
- Promote an integrated information lifecycle Force-wide; and
- Ensure that the Force infrastructure and processes can provide the right information to the right people at the right time for the right purpose.

To achieve the above, the Force will be guided by the following standards, which reflect the fundamental information management values of the Force.

3. Information Management Values

3.1 The Standards, which require:

- Recording of information to comply with the principles of the National Intelligence Model (NIM);
- Appropriate classification, grading and recording of police information;
- The eradication of unnecessary duplication;
- The highest quality of information;
- Proper evaluation;
- Appropriate audits to be undertaken;
- Risk Management processes to be employed; and
- Appropriate vetting to be undertaken.

3.2 Business Management, which involves:

- The duty to obtain and manage information;
- Compliance with the National Intelligence Model (NIM);
- Cost effectiveness in information management;
- Commitment to an information culture; and
- Recognising information as a business asset and the value of information used in decision making and program management.

3.3 People Management, which involves:

- The ownership of information;
- Users responsibilities towards information;
- Competency in handling information; and
- Investment in appropriate resources, skills and training.

3.4 Information Sharing, which includes:

- The duty to share information lawfully;
- Providing the right information for the right person/people at the right time for the right purpose;
- The protection of sensitive information and sources; and
- The need to address the obligations of those receiving information.

3.5 Data/Information Management, which includes:

- The review, retention and disposal of information;
- Conformity/compliance with external agreements;
- The use of appropriate information technology;
- The security of information;
- The aggregating of data;
- The storage of information;
- Complying with the Data Protection Act 1998;
- Complying with the Freedom of Information Act 2000; and
- Complying with the ACPO Information Systems Community Security Policy (CSP).

4. Scope of Strategy

- 4.1 This strategy mandates the areas that are identified under MoPI CoP and should also be used as good practice for all other information.
- 4.2 It applies to all information received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by all staff employed by the Force in the course of carrying out their duties. This document covers all formats of information including electronic, digital and hard copy.
- 4.3 This strategy does not redefine organisational structures, nor determine technology-based solutions; however, it will inform future technical developments.

5. Governance

The Force will establish the necessary strategic information management board(s) and develop key information management roles and responsibilities in order to comply with the MoPI Code and Guidance.

6. Responsibilities

- 6.1 The Force has a corporate responsibility to own and manage all information created, received and held for a policing purpose in accordance with the regulatory environment. The person with overall responsibility for this strategy is the Chief Constable.
- 6.2 The Force has a corporate responsibility to ensure it has a business continuity plan in place to safeguard its corporate and information assets.
- 6.3 The person(s) responsible for information management in the Force will:
- ensure that the IMS is available for all staff, partners and public to view;
 - ensure the integrity of the information;
 - give guidance for good information management practice and will promote compliance with this strategy so that police information will be:
 - a) accessed easily, appropriately and in a timely manner;
 - b) processed for a policing purpose;
 - c) shared and disclosed lawfully.
- 6.4 All individuals within the Force will ensure that all information created, received and held for which they are responsible, is accurate, relevant and kept up to date, and that decisions about it are properly recorded, thereby ensuring accountability with an accurate audit trail.

7. Relationship with Existing Policies

This strategy has been drawn up within the context of:

- MoPI (CoP);
- MoPI Guidance;
- Links with other legislation, statute and common law, regulations or national procedures affecting the Force **(See Part 2, Appendix A)**.

8. Relationship with Future Policies

All relevant future policies will be written with due regard to this strategy.

NB: This strategy must be read and implemented in conjunction with Force information management procedures and processes.

9. Equality Impact Assessment

An Equality Impact Assessment has been completed for this strategy. As a result of this assessment, it has been graded as having a low potential impact.

Part 2: Information Management Standards and Operating Procedures

1. Introduction

2. Information in a Policing Context

3. Regulatory Environment

4. Strategic and Operational Information Management

4.1 Citizen-focused Service Delivery

4.2 Governance

4.3 Effective and Lawful Use of Information

4.4 Information as a Force Asset

4.5 Information as a Shared Resource

4.6 Infrastructure and Strategic Management of Information

5. Governance Structure

6. Functions and Responsibilities

6.1 Programme Board

6.2 Executive

6.3 Chief Information Officer

6.4 Senior Information Risk Owner

6.5 Force Information Officer

6.6 Records Manager

6.7 Force Data Protection Officer

6.8 Force Freedom of Information Officer

6.9 Force Information Security Officer

6.10 Disclosure Manager

6.11 Business Process/Systems Owners

6.12 BCU Commander/Head of Department

6.13 Supervisors

6.14 All Staff/Users

7. Audit and Compliance

Appendices

A. Regulatory Environment

B. Key Definitions

Kent Police

Part 2

Information Management Standards and Operating Procedures

1. Introduction

1.1 Police information management cuts across all police business activities. It is critical that a coordinated and cohesive approach is taken to improve police performance in support of the following Force objectives:

- the Force will identify all business areas where police information is held and will maintain suitable information asset registers;
- information and intelligence will be collected in line with Force intelligence requirements and in accordance with the NIM;
- the Force will undertake business analysis to identify the relationship between police information held within different business areas;
- information will be managed to support business processes, including the relationship between different business areas;
- information will be accurate, up-to-date and readily accessible to those who have authority to see it;
- information will only be retained where necessary;
- information will only be disclosed or shared where lawful and necessary;
- a consistent approach to managing information will be adopted across the whole Force based on the lifecycle of information and having taken due regard of the MoPI guidance for Review, Retention and Disposal (RRD);
- methods of information management will be secure, protected, legal, and subject to environmental and proportional cost issues;
- both general and more specialist, role-specific, training will continue to be provided in order to maintain the principles of this strategy.

- 1.2 Kent Police are committed to the information/record management principles defined by the International Standards Organisation (ISO) 15489, as follows:
- decide what records need to be created and what should be included in them;
 - decide the format and structure of the records, and the technology used to create and capture them;
 - decide about metadata creation and management, including persistent linkage between records;
 - identify use requirements;
 - decide what records to keep, why and for how long;
 - decide how to organise the records;
 - identify the organisational risk of not maintaining records;
 - ensure safe storage, effective delivery and preservation over time;
 - comply with legal policy, organisational needs and relevant standards; and
 - evaluate and improve the processes.
- 1.3 These standards provide an opportunity for achieving national consistency through complying with the MoPI CoP by:
- ensuring the Force understands the value of information and is able to exploit it as a corporate asset;
 - providing the standards for information management in respect of definitions, data standards and the rules for disclosing/sharing;
 - integrating all Force policies and protocols relating to, and in the context of, managing police information; and
 - putting in place cost effective mechanisms to ensure the Force and its partners have access to the right information, in the right form, at the right time.
- 1.4 Each business area will have a named business/system owner of information who will be responsible for its creation and accuracy; and a custodian of information (responsible for its physical safekeeping). All Force systems will be formally security accredited in line with the ACPO Community Security Policy and associated Force policies.

2. Information in the Policing Context

- 2.1 Information will be managed corporately and will have common standards applied to it (as defined by MoPI Guidance), in order for it to be used for a policing purpose. This will enable the Force to agree solutions to information management issues locally and nationally.
- 2.2 Force policies and procedures for all key elements of information management will comply with MoPI CoP and other legislative regulations, (see **Appendix A**) policies and standards affecting the management of information functions across all Force business areas.
- 2.3 New systems (and where possible, legacy systems) will be integrated and information received or collected will be entered into the system once as part of the operational process at the point of service delivery, without intervening manual processes. This requirement will form part of the new system accreditation process.

3. Regulatory Environment

MoPI CoP exists within a regulatory environment that includes statutes, common law, codes and guidance. Please see **Appendix A** for a detailed list of regulations.

4. Strategic and Operational Information Management

The Force will address key focus areas as follows:

4.1 Citizen-focused Service Delivery

- 4.1.1 The Force will provide a citizen-focused service that responds to the needs of its communities and individuals through building effective links with its local communities and members of the public to ensure their needs are met.
- 4.1.2 The Force will implement integrated information management processes across all business areas and activities to enable it to bring about increasingly responsive services to its local communities and individuals.
- 4.1.3 The Force will work in partnership with local authorities and other organisations in providing a safer environment for its citizens.

4.2 Governance

- 4.2.1 The Force has a duty to obtain and manage information needed for a police purpose.
- 4.2.2 All information will be evaluated and processed within an acceptable time period defined by a strategic information management board and included in Force Policy.
- 4.2.3 The Force will manage its information with due regard to the different types of information it is legislatively bound to hold.
- 4.2.4 Information will be held where and when it is considered that it is necessary for a police purpose and assessed for reliability.

- 4.2.5 Information originally recorded for police purposes will be reviewed in line with MoPI Guidance and compliant with the principles of DPA 1998.
- 4.2.6 When it is reviewed, information originally recorded for police purposes will be considered for retention or disposal.
- 4.2.7 There are certain public protection matters which are of such importance that the Force will only delete the information if:
- the information has been shown to be inaccurate, in ways which cannot be dealt with by amending the record; or
 - it is no longer considered that the information is necessary for police purposes.
- 4.2.8 The decision to retain information can be approved by a Supervisor at any level.
- 4.2.9 Disposal of records will have due regard to the MoPI National Retention Assessment Criteria (NRAC) as defined in Force Policy and as agreed by Chief Officers.
- 4.2.10 A record of all reviews and disposals will be maintained electronically by systems, wherever possible and having due regard to the MoPI guidance.
- 4.2.11 The Force is committed to improving and maintaining a fit for purpose flow of information, central to its ability to function effectively and efficiently, and to ensuring that staff are aware of the Force's key aims, objectives, strategies and developments.
- 4.2.12 All Force information will be processed in accordance with the latest ACPO Information Systems Community Security Policy (CSP).
- 4.2.13 A process of regular monitoring for the accuracy, adequacy, relevancy and timeliness of Force information is established, which includes dip sampling of records within each business area.
- 4.2.14 Regular, independent inspections and audits of local staff monitoring processes will be undertaken.
- 4.3 Effective and Lawful Use of Information
- 4.3.1 The Chief Information Officer (ACPO) is responsible for ensuring recording procedures are established in accordance with MoPI Guidance to enable information to be as complete and accurate as possible.
- 4.3.2 The Force is committed to continual development of information processes to enable effective information sharing partnerships, and ensure disclosure and dissemination in a lawful manner.
- 4.3.3 The Force is committed to providing an environment to support staff in their role of managing the lifecycle of the information.
- 4.3.4 Where appropriate, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information will be recorded to permit later review, reassessment and audit.

4.3.5 The format in which the information is recorded will comply with standards agreed and applied across the police service to facilitate exchange of information and processing within standard police technical systems.

4.4 Information as a Force Asset

4.4.1 Each Force business area will have a defined business process owner who will be responsible for the information's lifecycle processes and consistency of those processes across the Force.

4.4.2 All information will have a defined custodian who will be responsible for its management and for making it accessible to those who need it in a secure and timely manner under central guidance/authority.

4.4.3 The Force will maintain and develop the quality of facilities and equipment relevant to information provision.

4.5 Information as a Shared Resource

4.5.1 The Force will ensure information is accurate, reliable and up-to-date, and available to any other police Force as specified in the MoPI CoP requiring information for police purposes provided that the chief officer responsible for the record is satisfied that the police Force seeking access to the information applies the principles set out in the MoPI CoP.

4.5.2 The Force will have in place appropriate agreements for sharing information (Information Sharing Agreements), which will be stored in a central register.

4.5.3 Special procedures will be applied to a request for access to information recorded for police purposes, in particular, where it is necessary to protect the source of sensitive information or the procedures used to obtain it.

4.5.4 In making national or local agreements and protocols for the sharing of police information with persons or bodies other than police Forces where a power to share exists, or in responding to individual requests for information outside such agreements or protocols, the Chief Officer will require those to whom information is made available, to comply with the following obligations:

- Police information made available in response to such a request will be used only for the purpose for which the request was made;
- If other information available, at the time or later, to the person or body requesting police information tends to suggest that police information is inaccurate or incomplete, they will at the earliest possible moment inform the Force of such inaccuracy or incompleteness, either directly or by reporting the details to the relevant Business Process/System Owner (BPO). The BPO responsible for the police information concerned will then consider, and if necessary, record any additions or changes to the recorded police information.

4.6 Infrastructure and Strategic Management of Information

- 4.6.1 The Force is committed to a consistent approach to the strategic management of information at all levels.
- 4.6.2 The Force has a corporate responsibility for ensuring an appropriate information management infrastructure is implemented and maintained, including developing robust, reliable, flexible, scalable and secure systems for both electronic and paper-based records/documents.
- 4.6.3 The infrastructure will host integrated systems to provide seamless access to related information across different functional systems e.g. electronic automated systems to manage time and labour intensive activities internally and externally and it will be developed to accommodate existing and emerging business processes.
- 4.6.4 Business process owners will be responsible for developing strategic liaison between departments to facilitate coherent development of information provision.
- 4.6.5 As the Force becomes increasingly dependent on electronic information systems for its effective operation, the Force will ensure these systems do not suffer major periods of unavailability, and business continuity plans will be developed by business area owners in partnership and consultation with the Information Technology Department, informed by realistic risk assessments.

5. Governance Structure

The Force will adopt a similar structure to that presented within the MoPI Code and Guidance, as detailed in the following section (Note: a role can cover more than one function and some functions and responsibilities can be covered by multiple roles).

6. Functions and Responsibilities

As a matter of policy and procedure, all Force staff must understand their responsibilities when using or communicating personal or other data and information. In practice, everyone working for, or with, the Force who receives, creates, maintains, stores, reviews, discloses/shares or disposes of information, has a common law duty of confidentiality. This responsibility is established at, and defined by, law.

In addition to individuals' responsibility for information management, there are core levels and functions that have been identified to ensure that police information is managed effectively, efficiently and lawfully. Each of these has a different combination of responsibilities but some are shared:

6.1 Strategic Information Management Board (or equivalent ACPO level board)

6.1.1 The Information Management Board will deal with strategic issues surrounding information management in line with this IMS.

6.1.2 The Board will determine the organisation's policy for information assets and identify how compliance with that policy will be measured and reviewed, including:

- identification of information assets and the classification into those of value and importance that merit special attention and those that do not;

- quality and quantity of information for effective operation ensuring that, at every level, the information provided is necessary and sufficient, timely, reliable and consistent;
- the proper use of information in accordance with applicable legal, regulatory, operational and ethical standards and the roles and responsibilities for the creation, safekeeping, access, change and disposal of information;
- the protection of information from theft, loss, unauthorised access, improper use, including information which is the property of others; harnessing of information assets and their proper use for the maximum benefit of the organisation including legally protecting, licensing, re-using, combining, re-presenting, publishing and destroying;
- strategy for information systems, including those using computers and electronic communications and the implementation of that strategy with particular reference to the costs, benefits and risks arising;
- identifying and actioning the appropriateness of a central oversight role for all information held by the Force.

6.1.3 The Board will be responsible for ensuring information management training is identified.

6.1.4 Any issues which may impact on Force compliance with the CSP will be referred to the Senior Information Risk Owner (SIRO).

6.1.5 Membership of the Board will be determined by the Chief Information Officer (CIO) as Chair of the Board.

6.2 Executive

6.2.1 The Chief Constable has ultimate ownership of the Force IMS.

6.2.2 The Chief Constable is the Force Data Controller, in line with the Data Protection Act 1998 (DPA), and as such he has the duty to comply with the data protection principles, including, but not limited to, the following:

- determines why, as well as how, personal data including sensitive personal data, is to be processed and what security measures will be appropriate;
- has a duty to ensure that the collection and processing of any personal data within the Force complies with the data protection principles;
- retains full responsibility for the actions of any data processor used; and
- notifies all processing operations that involve personal data to the Information Commissioner and keeps this notification up-to-date.

6.2.3 The role of Data Controller is a primary legislative function, therefore, the role cannot be delegated, but he can appoint someone to manage the processes on his behalf (Force Data Protection Officer).

- 6.2.4 The Chief Constable has overall executive responsibility for management and use of information within Kent Police.
- 6.2.5 The Chief Constable will ensure that the Force adopts policy, procedures and processes for the management of information, and support their application force-wide so that information is used effectively for police purposes and in support of consistent national standards.
- 6.3 Chief Information Officer (CIO)
- 6.3.1 The CIO holds responsibility for the management of police information and as such has responsibility for overseeing all related functions for the management of police information such as Data Protection, Freedom of Information and disclosure/sharing which may be undertaken by separate internal departments, including agreeing what information can be shared, how and when, and countersigning Information Sharing Agreements (ISAs). The CIO must be at a suitable senior management level to decide the strategic direction of the Force in all information management matters.
- 6.3.2 The responsibilities of the CIO include, but are not limited to:
- Ensuring:
 - Force processes and systems adhere to the MoPI CoP, Guidance and Threshold Standards;
 - the IMS is maintained;
 - all ISAs are held and managed centrally within Force;
 - the process of sharing information is adhered to by both those in a supervisory and user capacity;
 - Force policies are appropriate to make certain that information is easily accessible and searchable;
 - the Force meets national requirements for the management of police information;
 - Operating Rules for all Force systems are available to all staff;
 - reporting lines exist to allow BCU Commanders or Department Heads to raise issues to Force Information Officer/s (or equivalent) if necessary;
 - reporting lines exist to allow Force Information Officer/s (or equivalent) to discuss matters (their own or those raised by BCU Commanders/Department Heads) at an ACPO level;
 - systems and processes are sufficient to effectively co-ordinate all staff roles involved with the management of police information;
 - appropriate role/function is available to represent the Force at named forums.

- Overseeing:
 - the management of all the Forces information assets and can demonstrate effective linkages between the different functions e.g. IT, Data Protection etc.
 - management of Freedom of Information matters (including compliance with the ACPO Freedom of Information Manual);
 - compliance with the latest ACPO Information Systems Community Security Policy (CSP);
 - all system responsibilities within the Force.
- Supporting staff to share information appropriately.
- Authorising ISAs.

6.4 Senior Information Risk Owner (SIRO)

- 6.4.1 The Force will have a Senior Information Risk Owner (SIRO) at ACPO level, to comply with CSP.
- 6.4.2 The SIRO has responsibility for understanding how the strategic business goals of the Force may be impacted by information management systems failure.
- 6.4.3 The SIRO is responsible for ensuring that information risk management and management processes are established and adhered to Force-wide.
- 6.4.4 The SIRO will make the final decision in cases where the ISO identifies potentially unacceptable residual risks during the systems accreditation process.
- 6.4.5 This is a strategic responsibility, which will not be confined to information technology or information assurance departments.

6.5 Force Information Officer (or equivalent)

The responsibilities detailed below may be undertaken by the function of an FIO or other title depending on the particular requirements of the Force. Typically over-seeing an Information Management team of staff an FIO may be responsible for:

- quality-assuring information sharing agreements (ISAs);
- monitoring compliance with relevant legislation;
- liaising with information owners and other stakeholders in the process;
- liaising with BCU Commanders/Department Heads when necessary to provide guidance and support on information management;
- providing advice and training on good practice;

- identifying officers or police staff able to handle requests that come into the organisation for information sharing;
- ensuring that Information Sharing Agreements are published on the Force intranet;
- maintaining a central register of existing Force ISAs;
- reporting on a regular basis to the Chief Information Officer or equivalent;
- identifying where there may be a need for a Force wide approach to sharing requests;
- supporting staff to share information appropriately;
- auditing, on an ad-hoc basis, the decision to share made by users, including the necessity, accuracy and adequacy of information shared;
- checking whether the decision to share meets a policing purpose or other legal duty or power;
- ensuring that information being shared does not compromise any police operation or the safety of others;
- ensuring that a risk-assessment process is adhered to by the user when making a decision to share information;
- ensuring that ISAs are reviewed in accordance with Force policy;
- providing feedback to staff on their performance;
- ensuring that MoPI Guidance, other relevant ACPO policy and guidance are disseminated and adhered to Force-wide.

6.6 Records Manager

The Force will have a designated records manager or equivalent who will:

- provide a single point of contact to process owners;
- ensure that the records management policy and standards are kept up-to-date and relevant to the needs and obligations of the Force, through consultation and assessment against external standards;
- ensure review, retention and disposal schedules are implemented
- conduct local quarterly review and evaluation of their systems registers to ensure accuracy and completeness;
- ensure that all registered files are available for those with authorised access;

- determine records management relationships with internal and external stakeholders, including audit and management teams;
- ensure that management teams supervising divisional/departments records management have the necessary skills and competencies;
- manage the storage conditions of all records on-site and off-site including contract storage services;
- monitor individual and Force compliance with the records management policy and standards.

6.7 Force Data Protection Officer

The Force data protection officer's responsibilities include:

- managing the Chief Officer's statutory obligations in respect of the DPA including; notification of processing to the Information Commissioner; compliance with the Data Protection Principles and securing individuals rights under the Act, including subject access requests;
- maintaining an up to date knowledge of, and advising on relevant legislation and general developments in data protection and related matters;
- promoting awareness of data protection matters through training, policy development, advice and guidance;
- undertaking systematic auditing and monitoring of information and systems in accordance with the ACPO Data Protection Manual of Guidance Part II: Audit;
- ensuring information and systems comply with the relevant legislation including the DPA;
- ensuring that appropriate security arrangements exist to protect information, including where necessary that suitable contracts are drawn up relating to the processing of police information by third parties;
- investigating and resolving complaints made in relation to the handling of personal information (in relation to data protection);
- assisting where appropriate in the investigation of disciplinary and criminal matters relating to data protection;
- liaising on all data protection matters between the Force and relevant regional or national bodies (including the ACPO Data Protection and Freedom of Information Portfolio Group and the Information Commissioner's Office);
- liaising with BCU Commanders/Department Heads when necessary to provide guidance and support on data protection matters;
- ensuring that the ACPO Data Protection Manual of Guidance Part 1: Standards are disseminated and adhered to Force-wide;
- liaise directly with the Chief Officer;

- liaising regularly with the Force Information Security Officer or equivalent.

6.8 Force Freedom of Information Officer

The Freedom of Information Officer's responsibilities include:

- managing the Force obligations in respect of the Freedom of Information Act 2000 (FoIA) including the Force publication scheme and requests for information under the Act;
- maintaining an up to date knowledge of, and advising on relevant legislation and general developments in freedom of information and related matters;
- ensuring that the ACPO Freedom of Information Manual is disseminated and adhered to Force-wide;
- promoting awareness of Freedom of Information matters through training, policy development, advice and guidance;
- liaising with BCU Commanders/Department Heads when necessary to provide guidance and support on Freedom of Information matters;
- liaising on all FoIA matters between the Force and relevant regional or national bodies (including the ACPO Data Protection and Freedom of Information Portfolio Group and the Information Commissioner's Office).

6.9 Force Information Security Officer (ISO)

The Information Security Officer's responsibilities include:

- acting as the point of contact for all information security issues;
- implementing organisational structures, policies, procedures and risk management programmes with respect to security matters;
- providing advice on the correct and secure operation of information processing systems and applications;
- ensuring appropriate security measures are in place for procedures and technical measures to prevent unauthorised or accidental access to, amendment of, or loss of police information;
- quality assuring local information security policy documentation;
- demonstrating an approach to implementing security that is consistent with national and local requirements;
- marketing the need for information security;
- providing advice on security education and training;

- co-ordinating all investigative and reporting action that may be undertaken into actual and suspected incidents of security significance;
- co-ordinating and advising on the implementation of specific security requirements for new and legacy systems and services, and leading on the local systems accreditation process;
- establishing and ensuring that third party agencies sharing, accessing, storing or processing information and information assets owned by the Force, comply with the defined threshold standards;
- maintaining appropriate contacts with other community members, Government departments and regulatory bodies;
- liaising with BCU Commanders/Department Heads when necessary to provide guidance and support on information security matters;
- reporting on a regular basis to the CIO or equivalent; representing member interests at a Regional and National level on information security issues;
- ensuring appropriate security measures are afforded to information, including personal data, thereby assisting Forces' compliance with the DPA in order to discharge security responsibilities;
- liaising on all Information Security matters between the Force and relevant regional or national bodies (including the ACPO Information Security Portfolio Group).

6.10 Disclosure Manager

6.10.1 The Disclosure Manager or deputies to act as a central point of contact with responsibility for ensuring:

- all requests for, and disclosure/sharing of, information are carried out in accordance with Force ISAs and with due regard to all relevant legislation and guidance including the ACPO/CRB QAF;
- all information received is conveyed, handled and kept in a confidential and secure way and, if not disposed of, returned to the originating agency when it is no longer required;
- maintaining and managing the designated officers register/list and informing the relevant business area/activity managers responsible for nominating designated officers of the requirement to replace any designated officers who have ceased to be involved in that role.

6.10.2 Under the CRB service level agreement (SLA) with ACPO and individual police Forces, each Force will provide a Force Delivery Manager (FDM) who will be the single point of contact for CRB matters.

6.11 Business Process Owner/System Owner (BPO)

6.11.1 Each business area will have a designated BPO, at senior management level, with whom the ownership of the business systems and processes and the collection and disposal of information lies.

6.11.2 The BPO is responsible for ensuring the information risk management processes within their business area are in line with the SIRO's directives.

6.11.3 The BPO is responsible for the creation and accuracy of the information within their business area.

6.11.4 The BPO will:

- define the service levels needed from any information and records management process;
- ensure that the information management processes meet the best practice requirements for their business area and for the Force as a whole;
- ensure there is the ability to link and cross-reference information across the different business areas including strategic liaison between departments to facilitate coherent development of information provision;
- ensure that the system is operated in compliance with its accreditation documentation, including its purpose, functionality, access rights and user operating procedures, and that any need for change is formally managed;
- provide a process for recording decisions to share or not to share information;
- set information and individuals access status;
- take active responsibility for information management and for ensuring that all staff are involved in the practice and implementation of the information management strategy. This will encompass:
 - internal communications, profile raising and publicity;
 - appropriate resources including training;
 - resilience of continuity and consistency of function and responsibility;
 - review of procedures and implementation plan for specific actions arising;

6.11.5 In relation to review, retention and disposal, the BPO will:

- ensure that the process for reviewing records is clearly communicated and in accordance with MoPI guidance and associated Force Policy;
- authorise the outcome of all process reviews conducted in their area of responsibility;

- ensure that the level at which decisions to retain and dispose of all groups of records are taken, is in compliance with Force policy;
- ensure quality assurance monitoring of records held by their department/area is undertaken regularly and at least annually;
- ensure staff responsible for undertaking reviews are trained in accordance with the MoPI National Training and Delivery Strategy.

6.12 BCU Commander/Department Manager

The responsibilities of a BCU Commander or Department Manager, with regards to information management include:

- ensuring the BCU or department under their command complies with all Force policies, legislation, procedures and processes relevant to information management;
- liaising and raising issues with the Force Information Officer or equivalent, Force Data Protection Officer, Force Freedom of Information Officer or Force Information Security Officer where necessary to seek advice and to ensure information is shared appropriately within the boundaries of Force and National policy and legal framework;
- ensuring data quality is treated as a priority;
- ensuring staff are recording information in the appropriate format;
- ensuring staff responsible for recording, and undertaking reviews of police information are trained in accordance with the MoPI National Training and Delivery Strategy.

6.13 Supervisors

Supervisors will have a key role in quality assuring the management of police information. Their responsibilities include:

- perform regular dip samples of records created in their business area;
- ensure information is recorded in the appropriate format and ensure feedback to staff on performance provided;
- overseeing the quality assurance process for accuracy, adequacy, relevancy and timeliness;
- monitoring ad hoc decisions to share;
- ensure risk assessment process is adhered to by the user when making decision to share;
- ensure ISAs are reviewed in accordance with Force policy;

- ensure users of systems are aware of, and adhere to, Force policies and procedures relating to information management and systems;
- provide briefings and tasking on information collection;
- provide opportunities for debriefing operations;
- ensure correct processing of 5x5x5s.

6.14 All Staff/Users

6.14.1 All staff involved in the management of police information or who have access to personal data have individual responsibilities as detailed below:

- to apply the basic principles of effective information management (as contained within the MoPI CoP, Guidance and associated Force policy);
- to recognise the value of confidentiality and information security and the dangers of inappropriate sharing of police information;
- to recognise the value of sharing and disclosing information and the dangers of failing to share when the circumstances require it;
- to be aware of the current intelligence requirements; to ensure that information is collected for a policing purpose;
- to record information in the appropriate format;
- to record information in compliance with the recording and data quality principles;
- to disseminate information where appropriate;
- to apply operating rules relevant to business areas to which they have access;
- to apply rules relating to information security including applying protective marking to the information being shared under the GPMS;
- will only share in accordance with agreed procedures;
- to ensure compliance with all relevant legislation including the Human Rights Act 1998, Data Protection Act 1998 and Freedom of Information Act 2000.

6.14.2 All staff responsible for creating records will:

- ensure person records are unique;
- quality assure the recording of the 5x5x5 and ensure the linking together of information where relevant; to identify opportunities for analysis of series or linked events;

- establish and enter the relevant MoPI NRAC grouping for a record at the point of its creation;
- document the provenance of information recorded;
- assess the information to identify and prioritise actions.

6.14.3 All staff responsible for reviewing records will:

- follow Force policy in relation to the implementation of MoPI NRAC when reviewing records, to determine their continued necessity for a policing purpose;
- document the review process as described in Force policy, wherever there is no automated mechanism in place; and
- ensure that information to be disposed of is not duplicated, and therefore retained, elsewhere.

7. Audit and Compliance

7.1 The Force Compliance Auditor(s) will be responsible for ensuring day-to-day operation of internal compliance initiatives to ensure that information management policies, procedures and processes are followed, data quality standards are met and benefits are realised. It is important that coordination takes place that includes:

- ensuring that information management policies and procedures are being communicated to appropriate Force personnel and are being adhered to;
- monitoring use of shared/personal storage space;
- ensuring that metadata exists for all documents and files;
- monitoring the use of the Force file management systems and processes, including appropriate naming and assigning of metadata for all documents and folders;
- ensuring that appropriate data standards and targets are in place and met;
- ensuring that appropriate paper filing takes place;
- ensuring that the accuracy of data is regularly assessed;
- working with the security and records management teams to define and prioritise a continuous audit programme, based on high risk areas.

7.2 The Force Compliance Auditor(s) will have responsibility for ensuring regular information quality assurance audits across business areas. This will include:

- establishing a structured and organised audit mechanism, including processes, methodology, timescales, reporting and follow-up;

- setting compliance criteria in accordance with accredited standards and in consultation with key information management post holders;
- overseeing the whole audit process.

7.3 Audit and compliance will be based on the information governance concerned with the standards that apply when information is processed i.e. how information is held, obtained, recorded, used and shared.

Regulatory Environment

- Police Act 1997 (Part V)
- Freedom of Information Act 2000 and the Code of practice on records management as raised under s46 of the FOIA
- Criminal Justice Act 2003
- Crime and Disorder Act 1998
- Serious & Organised Crime & Police Act 2005
- Sexual Offences Act 2004
- Limitation Act 1980
- Criminal Procedures & Investigations Act 1996
- Data Protection Act 1998
- Children Act 1989
- Children Act 2004
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Domestic Violence, Crime and Victims Act 2004
- Statutory Code of Practice on the Management of Police Information (2005)
- Guidance on the Management of Police Information (2010)
- Code of Practice on the NIM (2005)
- ACPO Community Security Policy
- ACPO Data Protection Manual of Guidance Parts 1 & 2: Standards & Audit
- ACPO (2005) Investigating Child Abuse and Safeguarding Children
- ACPO (2004) Investigating Domestic Violence
- ACPO (2004) Recording, Management and Investigation of Missing Persons
- MAPPA Guidance (2003)
- Manual of Guidance on the NIM (2005)
- ACPO Manual of Guidance: The Freedom of Information Act
- ACPO NIM Briefing Model (2003)
- CPS Disclosure Manual
- HMG Manual of Protective Security
- ACPO Guidance for the investigation of corruption in the police service (2003)
- ACPO Cabinet Retention Guidelines (2005)
- Home Office Circular 25/2003
- Home Office Circular 05/2005
- Home Office Circular 06/2006
- Computer Misuse Act 1990

Appendix B

Key Definitions

Data

Information which:

- a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- b) is recorded with the intention that it should be processed by means of such equipment;
- c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68. (Data Protection Act 1998); or
- e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d) (this fifth category was created by the Freedom of Information Act 2000 with effect from 01 January 2005).

The component(s) of information such as numbers, words or pictures without context, which in themselves - without any context - mean little and say even less. Data becomes information once it is put into a framework or structure that provides context.

Document

A structured unit of recorded information, published or unpublished, in hard copy or electronic form, and managed as a discrete unit. (ISO 15489:2001) A document forms part of a business transaction and is linked to other documents relating to that transaction or process.

Information

Data that has context and meaning and is, therefore, able to be understood by people.

Information Asset

A definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation, i.e. they are not easily replaceable without cost, skill, time, resources or a combination. The information which comprises an Information Asset, may be little more than a prospect name and address file; or it may be the plans for the release of the latest in a range of products to compete with competitors.

It is the purpose of information security to identify the threats against, the risks and the associated potential damage to, and the safeguarding of information assets. (Information Security Glossary: <http://www.yourwindow.to/information-security/>)

Information Lifecycle

The creation, acquisition, cataloging/identification, storage and preservation of, and access to, information.

Information Management	(IM) The function of managing the organisation's information as an asset, i.e. the provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decision making. This comprises the ability to know what information exists regarding a particular subject, where and how they are stored, ownership, and when they should be disposed of.
Metadata	Descriptive and technical documentation to enable the system and the records (that are described) to be understood and to be operated efficiently, and to provide an administrative context for the effective management of the records.
Record	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. (ISO 15489: 2001)
Records Management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (ISO 15489: 2001)