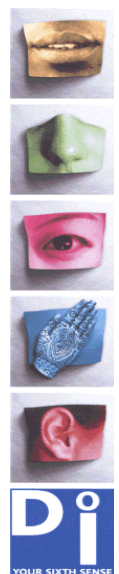




<b>Freedom of Information Act Publication Scheme</b>	
<b>Protective Marking</b>	NOT PROTECTIVELY MARKED
<b>Publication Scheme Y/N</b>	Y
<b>Title</b>	MPS Information Governance Framework
<b>Version</b>	V.1
<b>Summary</b>	Description of proposed framework for governance of MPS information
<b>Branch / OCU</b>	Dol 2(2) Information Strategy & Policy Development
<b>Date created</b>	24 September 2007
<b>Review date</b>	23 September 2010

<i>-Title &amp; Version</i>	MPS. Information Governance Framework. V.1
<i>Author</i>	Simon Theodorou
<i>Organisation</i>	DoI2(2) - Information Strategy and Policy Development.
<i>Summary/Purpose</i>	Description of proposed framework for governance of MPS information.

# INFORMATION GOVERNANCE FRAMEWORK



## Contents

Section	Title	Page
1	Introduction	2
2	Context	2
3	Benefits	3
4	Information Governance Framework Implementation	4
5	Summary of Roles and Responsibilities	6
6	Roles and Responsibilities	10
Appendix 1	Diagram	29
Appendix 2	Glossary	30

### 1. Introduction

- 1.1 This document proposes the establishment of a framework for the governance of all information owned by the Metropolitan Police Service (MPS). The MPS Information Governance Framework (IGF) introduces a formal governance structure with clear roles and responsibilities, thereby increasing ownership and accountability in the management of MPS information.

This framework has been designed to support strategic MPS corporate and national goals, most notably:

- The Code and Guidance on the Management of Police Information (MoPI) arising from recommendations 8 – 11 of the Bichard Inquiry Report into the police response to the Soham child murders.
- MPS corporate objective No 9 in MPS/MPA Key Control Framework – ‘continuous improvement in the management of information’.

### 2. Context

- 2.1 The Directorate of Information (DOI) sets corporate policy in respect of information. Corporate policy applies in general terms to all MPS information and provides a reference to ensure consistency in the setting of policy in business specific contexts.

- 2.2 As should be expected, not all information has the same business value nor carries the same risks, and specific rules need to be applied based on those values. Information can be grouped into 'collections'. A collection is defined as information gathered together for a particular purpose (e.g. Human Resources information, Criminal Intelligence). Proportionate rules specific to these collections and their value need to be set to ensure that MPS information is managed in its business context.
- 2.3 In particular, rules are required to provide management of a number of critical governance issues, such as:
- **Overall Accountability** - Providing corporate assurance to the Commissioner who has overall accountability for the governance of MPS information.
  - **Accessibility** – who may have access, how long access may be lost before it is restored, and how quickly it must be made available when required
  - **Quality** – accuracy and definitions of adequacy for business purpose
  - **Meaning** – decisions over the meaning/definition and structure of business information
  - **Risk Management** – management of risks involving MPS information and ownership of any residual risk after mitigation
  - **Authority** – Permitting the use of information for new purposes and/or by new groups of people
  - **Review & Disposal** – deciding on periods for the review of information against business need and ultimately for its disposal.
- 2.4 Whilst it is recognised that they are unlikely to be information management experts, the individuals best placed to understand the value of specific collections of information and to define the rules by which they should be managed are those whose business is most directly supported by them. There are benefits to greater clarification in the MPS over who those individuals are, what responsibilities they should exercise and the availability of expert information support that they can draw upon to advise and support them.

### **3. Benefits**

- 3.1 Introduction of this framework will assist in bringing a number of tactical and operational benefits to the MPS and to the citizens we serve. Key benefits from improved management of information include:

- More informed decision making with regard to deployment of financial and operational resources
- Better policing decisions which are auditable and more accountable
- Improved processes for joint agency working
- Improved data quality, leading to improved effectiveness in all areas of MPS business
- Increasing public/victim/witness trust in the way the MPS manages its information, leading to an increase in reporting of crime and increased provision of community intelligence.
- Satisfying the requirement within the Management of Police Information (MoPI) for an information management governance structure
- Meeting our legislative/external obligations, e.g. under data protection and freedom of information legislation
- Providing clarity and accountability in the management of MPS information

### 3.2 Future Policies and Policy/SOPs Reviews

In order to ensure that the MPS reaps these benefits, it is important that all relevant, future policies and Standard Operating Procedures (SOPs) will be written with due regard to this framework. Existing policies and SOPs must be reviewed with due regard to this framework.

## 4. Information Governance Framework Implementation

- 4.1 Whilst the driver for establishing the IGF comes from MoPI, the IGF will be a framework for all MPS information, not solely 'police information' as defined in the Code of Practice and Guidance<sup>1</sup>. Thus it includes things like CCTV, pictures and maps, as well as HR and Finance Systems. The framework is applicable to information held in all formats, not only that which is held electronically, but information held in paper or other hard copy form too. Thus, the governance framework will drive improvement in the management of all MPS information.

---

<sup>1</sup> MoPI defines police information as information that is required for policing purpose. The Code of Practice defines policing purposes as:

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

- 4.2 The next chapter provides an overview of the IGF, by identifying 'IGF roles' that should be adopted by the MPS. It is not envisaged that new posts be created but that the functions within each IGF role be included within existing specific job profiles. To be fully effective the IGF roles must, in due course, be linked to job competencies and personal development reviews.
- 4.3 If the IGF, as an approach, is formally approved at strategic level, the MPS MoPI team should proceed to plan for full implementation. Products are likely to include:
- Costings and a business case seeking the Resources required to implement the IGF, taken forward as part of the MoPI business case
  - Further consultation with those identified to carry out IGF roles to resolve any issues regarding the inter-dependencies between different IGF roles
  - Further consultation with Information Governors in order to reach agreement on aligning information sets with their logical Information Governors
  - Written guidance for individuals showing how IGF roles should be carried out and the dependencies between IGF roles (showing how they work together, and
  - Training programme to be developed to equip individuals with IGF roles with the requisite skills required to carry out their IGF functions.

## **5. Summary of Roles and Responsibilities**

### **5.1 The Commissioner**

5.1.1 The Commissioner is ultimately responsible for the effective management and use of information within the MPS. The Commissioner is also data controller for the MPS, as defined by the Data Protection Act 1998.

5.1.2 Underneath the Commissioner, governance of MPS information is divided into two distinct areas:

- The **Business Area** – those that are accountable for and utilise the information, and
- **Information Policy and Support** – information specialists that support those in the Business Area by providing policy, procedures and expertise for the management of MPS information.

### **5.2 The Business Area**

5.2.1 Members of the Management Board are the MPS **Information Governors**. They have responsibility and accountability for setting rules for the management of information (see 2.3) such as those that relate to creation/collection, accuracy, sharing, review and deletion of the information and for providing assurance to the Commissioner with regard to compliance with relevant legislation (e.g. Data Protection Act 1998, Freedom of Information Act 2000 and Human Rights Act 2000). These rules will be set within corporate information management policy and SOPs for which the Director of Information has responsibility. An Information Governor may delegate functions within their role, but they may not delegate their accountability. An Information Governor is concerned with 'information', not 'information systems'.

5.2.2 Every MPS system, whether 'electronic' or 'hard copy', that records, stores, or processes MPS information, must have a designated 'owner', known as an **Information System Custodian**. Information System Custodians are responsible for ensuring that their systems comply with the rules set by Information Governors in addition to corporate information management policy and SOPs. It is recognised that most systems store and use information from across more than one business area. Therefore Information System Custodians will have to ensure that their systems are compliant with the relevant Information Governor's rules and liaise with Information Governors in order to resolve any conflicts. Information System Custodians may delegate parts of their role, but this must be formally recorded and subject to review.

- 5.2.3 **OCU Commanders/Heads of Branches** will be responsible for ensuring that the OCU/branch under their command complies with all force policies, procedures and processes relevant to information management.
- 5.2.4 **Information Managers** are responsible for monitoring compliance with data quality and recording principles through regular quality reviews and reporting results back to local senior management through local performance indicators, and supporting Supervisors (6.6) in carrying out their supervisory functions.
- 5.2.5 **Supervisors** Line Management grades who supervise staff with regard to use of MPS information and information systems are responsible for ensuring that their staff are aware of their responsibilities (see 6.7) within this framework and comply accordingly.
- 5.2.6 **All Staff** involved in the management of police information or who have access to personal data are responsible for being familiar with, and adhering to legislative requirements and MPS policy, procedures and processes with regard to managing information. Individuals 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 are properly recorded, thereby ensuring accountability with an accurate audit trail. All staff should be aware of their duty of confidentiality.

### **5.3 Information Policy and Support**

- 5.3.1 This part of the IGF relates to information specialists, responsible for:
- Constructing an information governance framework
  - Setting corporate information management strategy, policy and Standard Operating Procedures
  - Providing information management guidance to those in the business area in specialist areas, such as information governance, information security, data protection, freedom of information, information sharing, records management and data management
  - Taking specialist decisions, especially around statutory requirements such as data protection, information sharing and freedom of information matters
  - Conducting inspections of compliance with information management policy and SOPs, and recommending corrective action as appropriate
  - Recording and reporting security incidents involving MPS information, non-compliance with information management policy and SOPs, and breaches of data

- protection, freedom of information and human rights legislation
- Measuring the quality of MPS data help to address the root cause of data quality, and

A number of the functions are specified in the MoPI Information Management Strategy Template, which will help the MPS to achieve compliance with the statutory Police Information Code of Practice. These specified functions have been incorporated into the framework, although they have not been included into specific role profiles as these are subject to change.

### **5.3.2 The Director of Information**

The Director of Information is the MPS Chief Information Officer with responsibility for the management of MPS information, including all related functions such as data protection, freedom of information, disclosure and sharing. As the Senior Information Risk Owner the Director of Information has responsibility for understanding how the strategic business goals of the MPS may be impacted by information management systems failure and ensuring that information risk management and management processes are established and adhered to. As a member of Management Board, the Director of Information is also an Information Governor.

### **5.3.3 Head of Information Compliance**

The Head of Information Compliance is responsible for ensuring corporate compliance initiatives to ensure that information management policies and processes are followed. Provides line management responsibility to the Information Security Officer and Head of Public Access Office.

### **5.3.4 Head of Records Management**

The Head of Records Management is responsible for ensuring effective file management systems and processes and ensuring that review, retention and disposal schedules are implemented in compliance with MoPI principles.

### **5.3.5 Information Security Officer**

The Information Security Officer is responsible for ensuring effective security measures are in place to protect MPS information assets.

### **5.3.6 Head of the Public Access Office**

The Head of the Public Access Office is responsible for managing the Commissioner's statutory obligations in respect of the Data Protection Act 1998, and Freedom of Information Act 2000.

### **5.3.7 Head of the Information Sharing Support Unit**

Working directly to the Head of the Public Access Office, The Head of the Information Sharing Support Unit is responsible for ensuring that MPS information is shared safely and within corporate information sharing rules.

### **5.3.8 Head of Data Management**

Responsible for management of corporate initiatives to define data standards, measure the quality of MPS data, assist in the improvement of data quality and in the development of amendment of new and existing systems.

### **5.3.9 Disclosure Manager**

Under Part V of the Police Act, 1997, the MPS is required to consider whether it holds any relevant information that ought to be disclosed in relation to persons seeking access to Children, Vulnerable adults and persons applying for gaming licences. The requests for these checks come from the Criminal Records Bureau (CRB) to the MPS Character Enquiries Centre (CEC). The CEC Disclosure Manager ensures that correct disclosure processes are established and followed.

## **6. Roles and Responsibilities**

### **6.1 The Commissioner**

6.1.1 The Commissioner has ultimate ownership and accountability for MPS information and executive responsibility for management and use of information within the MPS.

6.1.2 As force data controller, the Commissioner, in line with the Data Protection Act 1998 (DPA), has the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which s/he is the data controller, including 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 MPS complies with the data protection principles
- Retains full responsibility for the actions of data processors
- Notifies all processing operations that involve personal data to the Information Commissioner and keeps this notification up-to-date.

6.1.3 The role of data controller is a primary legislative function, therefore the role can only be delegated once by the Commissioner.

6.1.4 The Commissioner 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.

6.1.5 The Commissioner has responsibility for ensuring that a programme of information management training is delivered.

## **The Business Area**

### **6.2 Information Governor (Management Board)**

- 6.2.1 Information Governors are accountable for the business systems and processes, involved in the collection, storage, use and deletion of information.
- 6.2.2 Accountable for ensuring that the information management rules set are in line with processes, policy and SOPs set by the Director of Information and that business risk management processes are in line with the process set by the Director of Risk Management.
- 6.2.3 Accountable for the creation and accuracy of the information within their business area.
- 6.2.4 Information Governors will provide an annual written submission to the Commissioner with regard to the MPS Information for which they are accountable. This submission will consist of a brief outline of the current position and provide assurance to the Commissioner that the information is being managed effectively and risks to it are identified and managed.
- 6.2.5 Information Governors will be supported by information management professionals in order to:
- Define the service levels needed from any information and records management process
  - Be accountable for the resolution of information management issues affecting the information they are responsible for
  - 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 documentation is produced to define the purpose, functionality, access rights and user operating procedures and standards adhered to for the information for which they are accountable
  - Ensure protective marking is applied and recorded for all information (electronic and paper) and that access is managed by assigning specific access management roles to individual posts
  - Promote and ensure information management best practice is followed in their area of responsibility. This will encompass:

**Information Governance Framework - Version 1**

- a) internal communications, profile raising and publicity
- b) appropriate resources including training resilience and continuity of local roles and responsibilities
- c) review of procedures and addressing issues raised.

6.2.6 In relation to review, retention and disposal, the Information Governors will:

- Ensure that the process for reviewing records is applied and documented
- Authorise the outcome of all process reviews conducted in their area of responsibility
- Ensure quality assurance monitoring of records held by their department/area is undertaken in compliance with the Manual of Police Information, which will be incorporated into MPS Standards
- Ensuring staff responsible for undertaking reviews are trained in accordance with the MoPI National Training and Delivery Strategy and MPS Standards.

## **6.3 Information System Custodian**

6.3.1 Information System Custodians have responsibilities, which include assuming the Senior Responsible Officer role during the development/project phase of building a new system, ensuring that their systems(s), new or existing, comply with the rules set by Information Governors and appropriate MPS Standards.

6.3.2 Information System Custodians will:

- Oversee the development of new information systems, ensuring that they comply with the DOI project lifecycle. This function may be delegated, however accountability for the outcome may not
- In information system design, ensure that data quality of individual information sets is in accordance with the rules set by Information Governors
- During system development ensure that there is minimal duplication of input of data that has already been collected elsewhere
- During system development ensure that nominal records can be linked to records in other information systems
- Ensure that information systems comply with rules set by Information Governors
- Ensure that the review, retention and disposal schedule is implemented
- Develop and maintain System Operating Rules/Security Operating Rules
- Ensure that currently deployed systems comply with corporate information management policy and SOPs and the rules set by Information Governors. Where this is not the case an assessment of the risk of non-compliance must be carried out and any resulting recommendations formally considered and documented.
- Where appropriate, ensure that systems provide adequate management information on the level of compliance with Information Governors rules.

## **6.4 OCU Commander/Branch Heads**

6.4.1 The responsibilities of an OCU Commander or Branch heads, with regards to information management include:

- Ensuring the staff under their command comply with legislation and all MPS policies, procedures and processes relevant to information management. By so doing they will ensure OCU or department compliance with the MoPI CoP, Guidance and Threshold Standards
- Liaising with the Head of the Public Access Office, or Information Security Officer where necessary to seek advice and to ensure information is shared (including Criminal Records Bureau disclosure) appropriately within the boundaries of MPS and national policies and legal frameworks
- Raising issues on information management to the Head of the Information Sharing Support Unit, head of Public Access Office, Information Security Officer, Head of Information Compliance, or Head of Data Management as appropriate
- Ensuring staff are recording information in the appropriate system, in the appropriate format and to the agreed standards
- Ensuring that staff who are recording, and undertaking reviews of, police information are trained in accordance with the MoPI National Training and Delivery Strategy, and Information Governance Framework, and
- Identify a Single Point of Contact to discharge some of the above responsibilities, deal with quality assurance of information management and support Information Managers in their supervisory role.

## **6.5 Information Manager**

- 6.5.1 Working to the Single Point of Contact<sup>2</sup>/Quality Assurance Officer, or similar, Information Managers are responsible for monitoring compliance with data quality and recording principles through regular quality reviews and reporting results back to local senior management through local performance indicators.
- 6.5.2 Information Managers will promote good practice and provide support and guidance to Supervisors (see 6.6) in carrying out their supervisory functions over their staff (see 6.7 – All Staff).
- 6.5.3 Information Managers will liaise and investigate reasons for discrepancies between occurrences of data within their area and that of other areas.
- 6.5.2 Where there is no Information Manager in place to assume this role, it would normally fall to the Single Point of Contact/Quality Assurance Officer, or similar, to ensure that these functions are carried out.

---

<sup>2</sup> The Information Management Business Change (IMBC) team maintain a list of Single Points of Contact (SPOCs) to facilitate communication with business units and the tasking of their Information Managers. For more information about the SPOCs please visit the IMBC [Intranet site](#).

## **6.6 Supervisors**

- 6.6.1 Line Management grades who supervise staff with regard to use of MPS information and information systems are responsible for ensuring that their staff are aware of their responsibilities (see 6.7) within this framework and comply accordingly.
- 6.6.2 In particular they must conduct regular dip samples to ensure that staff record information, including information for a policing purpose (MoPI definition), promptly in the correct format, to the agreed standards and in the appropriate corporate system; and that the information is cross referenced across all business areas (where appropriate – i.e. the six MoPI business areas).
- 6.6.3 Introduce and oversee remedial measures recommended by the Information Manager/OCU commander/Branch Head (or SPOC) as a result of dip sampling.

## **6.7 All Staff**

6.7.1 All MPS staff 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 and Guidance) including the application of consistent processes and decisions, 'owning' and documenting decisions and changes, and working as part of a team
- 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, the controls necessary when sharing, and the dangers of failure to share when the circumstances require it
- To be familiar with, and adhere to force policy, procedures and processes when managing information
- To be aware of the current intelligence requirements, to ensure that information is collected for a policing purpose
- To record information in the correct format in the appropriate system, 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 all information being shared (electronic or paper based) and a risk assessment where the sharing is carried out with the partners in the voluntary or private sectors who do not have a statutory purpose to share information
- To share and disclose in accordance with agreed procedures
- Ensure compliance with relevant legislation including the Human Rights Act 1998, Data Protection Act 1998, Freedom of Information Act 2000, and Regulation of Investigatory Powers Act 2000.
- To report serious breaches of MPS information management policy and SOPs and non-compliance with relevant legislation

6.7.2 All staff responsible for creating records will:

- Ensure nominal 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
- Where possible, establish and enter the review date for a record at the point of creation
- Apply provenance to the information recorded, to apply relevant priority assessment if appropriate

6.7.3 When reviewing a record all staff will:

- Follow the National Retention Assessment Criteria (MoPI Guidance Appendix D(i) when iii) reviewing records to determine their continued necessity for a policing purpose
- Ensure that reviews are formally documented in hard copy format where there is no automated mechanism available and
- Ensure that information to be disposed of is not duplicated and therefore retained elsewhere by reviewing all information relating to a nominal at the same time.

## **Information Policy and Support**

### **6.8 Director of Information**

6.8.1 The Director of Information, or Chief Information Officer, holds responsibility for the management of information in the MPS, as well as for all related functions 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).

6.8.2 The responsibilities of Director of Information include the following:

a) Ensuring:

- MPS policy, processes and systems adhere to the MoPI Guidance and Threshold Standards; an MPS information strategy is established, maintained and promulgated throughout the Service, processes in place for managing the number and types of systems
- The development of all new systems follows the MPS DOI lifecycle and that new systems meet national standards, are compliant with the Information Policy Framework, MPS policy and Standard Operating Systems
- That every information set has an Information Governor and every system/application has an Information System Custodian
- That as Senior Information Risk owner, the impact of information management failures, or poor control mechanisms, on the strategic business goals of the MPS are understood. The Director of Risk Management will, on request, provide professional support to assist in the discharge of this responsibility
- The MPS information risk management processes are established, except for the MPS business risk management processes. The Director of Risk Management is responsible for ensuring that an MPS business risk management process is established that enables, inter alia, the management of information risks
- All information Sharing Agreements are held centrally within the MPS, and both meet the needs of the organisation and adhere to a corporate model

- The process of sharing information is adhered to by both those in a supervisor and user capacity
- MPS policies are appropriate to make certain that information is easily assessable and searchable
- The MPS meets national requirements for the management of police information
- Operating rules for all MPS systems are available to all staff
- Systems are sufficient to effectively co-ordinate all staff roles involved with the management of police information
- That the MPS is appropriately represented at named forums
- Reporting to the Commissioner/Management Board any serious instances of non-compliance with information management policy and SOPs and serious breaches of legislation with regard to information.

b) Overseeing:

- Management of data protection matters including compliance with the ACPO Manual of Guidance on Data Protection
- Management of freedom of information matters (including compliance with the ACPO Freedom of Information Manual)
- Compliance with the ACPO (2002) Community Security Policy (CSP)
- All system responsibilities within the MPS.

c) Supporting staff to share information appropriately.

## **6.9 Head of Records Management Branch**

6.9.2 The Head of Records Management has overall responsibility for records management policy and will:

- Have the appropriate cross-organisational authority to achieve key objectives
- Have responsibility for setting the criteria for risk assessment of records being undertaken by operational staff
- Conduct quality assurance reviews on records and processes
- Ensure that management teams and staff working within Records Management Branch have the necessary skills and competencies
- Manage any contract for off-site storage of hard copy records and associated processes and infrastructure
- Provide consistency of procedures in records management across the MPS, and liaise with colleagues in other forces on standards
- Monitoring use of shared/personal storage space
- Ensuring that metadata exists for all documents and files
- Monitoring the use of the MPS file management systems and processes, including appropriate naming and assigning of metadata for all documents and folders
- Ensuring that appropriate paper filing takes place

6.9.3 In relation to retention and disposal, the Records Manager will be responsible for:

- Ensuring quality assurance by monitoring of the records held by the business areas/departments/BCUs is undertaken
- Ensuring the review, retention and disposal schedule is implemented in accordance with MoPI principles.

## **6.10 Head of Data Management**

6.10.2 Responsible for ensuring day-to-day operation of corporate initiatives to measure the quality of data and compliance with corporate data management policies procedures and processes, the Head of Data Management is responsible for:

- Ensuring that appropriate data standards and targets are in place
- Ensuring that data quality is regularly assessed in compliance with the ACPO Data Protection Manual of Guidance
- Assist Information System Custodians with the provision of regular Data Quality Measurement reports
- Manage reporting of metadata, logical data models, data dictionary and constrained values
- Help to address the root cause of data quality problems,
- Advise on best practice to manage data, tackle data quality issues and develop/re-develop information systems
- Recommend to the MPS Information Authority with regard to approving the launch of new systems
- Maintain central repository of Information Governors and Information System Custodians.

## **6.11 Head of Information Compliance**

6.11.2 Responsible for ensuring day-to-day operation of corporate compliance initiatives to ensure that information management policies, procedures and processes are followed. It is important that co-ordination takes place that includes:

- Ensuring that information management policies and procedures are being communicated to appropriate MPS personnel and are being adhered to.

6.11.3 Responsible for ensuring regular information compliance audits across business areas. This will include:

- Establishing a structured and organised audit mechanism in compliance with the ACPO Data Protection Manual of Guidance, including processes, methodology, timescales, reporting and follow-up
- Setting compliance criteria
- Overseeing the whole audit process

6.11.4 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 obtained, recorded, held, used, retained and shared.

6.11.5 Appointing an Information Security Officer and Head of Public Access Office, to agreed national standards.

## **6.12 Head of Information Sharing Support Unit**

6.12.1 Reporting directly to the head of the Public Access Office, the head of the Information Sharing Support Unit is responsible for the management of the Information Sharing Support Unit:

- Quality assuring information sharing agreement documents (ISAs)
- Monitoring compliance with relevant legislation
- Liaising with stakeholders in the information sharing process
- Liaising with OCU Commanders/Departmental Heads when necessary to provide guidance and support on information sharing
- Providing advice and training on good practice
- Identifying officers or police staff able to handle requests that are received by the MPS
- Ensuring that Information Sharing Agreements are published on the MPS intranet
- Maintaining a central repository of existing MPS information sharing agreements
- Identifying where there may be a need to a MPS 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
- Assisting OCUs to ensure 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 MPS policy
- Ensuring that MoPI Guidance, other relevant ACPO policy and guidance are disseminated and adhered to MPS wide
- Defining MPS roles and responsibilities for information sharing agreements with other agencies.

## **6.13 Head of Public Access Office**

6.13.1 The Head of the Public Access Office is responsible for:

- Managing the Commissioner'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
- Managing MPS obligations in respect of the Freedom of Information Act 2000 (FoIA) including the MPS 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 data protection, freedom of information and related matters
- Promoting awareness of data protection and freedom of information matters through training, policy development, advice and guidance
- 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 with BCU Commanders/Department Heads when necessary to provide guidance and support on data protection and freedom on information matters
- Ensuring that ACPO Freedom of Information Manual and ACPO Manual of Guidance on Data Protection are disseminated and adhered to MPS wide
- Formally approving information sharing agreements
- Liaising on all Data Protection and freedom of information matters between the MPS and relevant regional or national bodies (including the ACPO Data Protection and Freedom of Information Portfolio Group and the Information Commissioner's Office)
- Liaising regularly with the Force Information Security Officer
- Liaising with the MPS Directorate of Legal Services with regard to advising on disclosure cases.

## **6.14 Information Security Officer**

6.12.1 The information security officer is responsible for:

- Acting as the MPS point of contact for 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 MPS 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
- Establishing and ensuring that third party agencies sharing, accessing, storing or processing information and information assets owned by the MPS, comply with the defined thresholds standards
- Maintaining appropriate contacts with other community members, Government departments and regulatory bodies
- Liaising with BCU Commanders/Departments Heads when necessary to provide guidance and support on information security matters
- Reporting on a regular basis to the Head of Information Compliance; 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 MPS' compliance with the DPA in order to discharge security responsibilities
- Liaising on all Information Security matters between the MPS and relevant regional or national bodies (including the ACPO Information Security Portfolio Group)

**Information Governance Framework - Version 1**

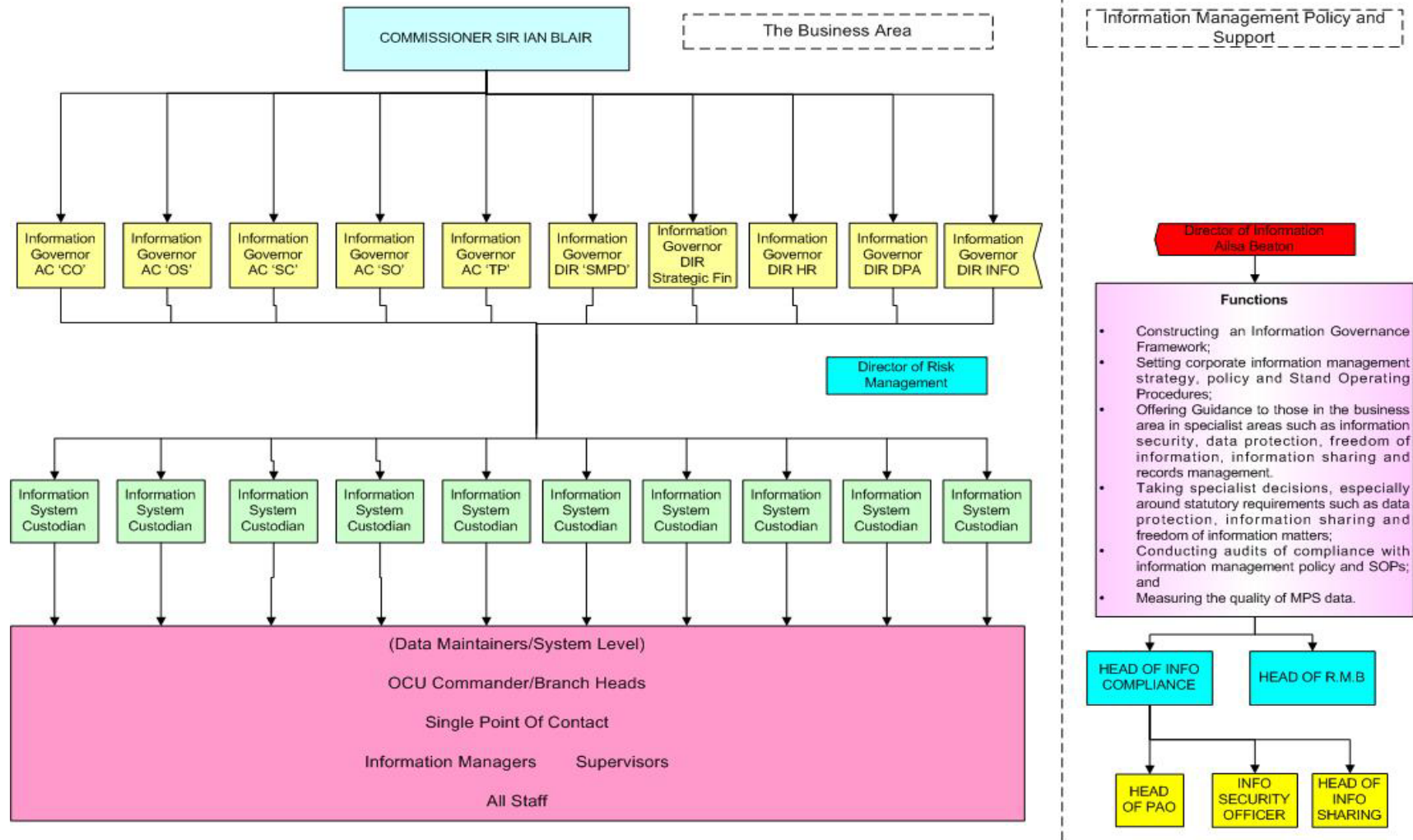
- Responsible for accrediting information systems with regard to risk, compliance with MPS Policy/SOPs on information management and information security and compliance with relevant legislation
- Responsible for facilitating the assessment of the residual risk affecting MPS information systems
- Ensure the Director of Information is aware of risk if deemed too great
- Day to day management of audits of compliance with information legislation, national guidance and MPS policy.

## **6.15 Disclosure Manager**

6.15.1 The MPS Disclosure Manager is responsible for;

- i) Criminal Records Bureau (CRB) Checks;
- ii) Ensuring that compliance with Part V of the Police Act, 1997, is evident;
- iii) Ensuring that an authority process is defined within MPS policy and adhered to;
- iv) Ensuring scheduled quality review processes are outlined in MPS policy and adhered to; and
- v) Compliance with the Quality Assurance Framework (QAF).

### Appendix 1 – Information Governance Framework - Diagram



## **Appendix 2- Glossary**

**CEC** – Character Enquiry Centre

**CRB** – Criminal Records Bureau

**DoI** – MPS Directorate of Information.

**Information Collection** - Information gathered together for a particular purpose.

**ISA** – Information Sharing Agreement

**IGF** – Information Governance Framework.

**MoPI** – Manual of Police Information.

**Police Information** – Information that is required for a policing purpose. (See footnote on Page 5).

**SOPs** – Standard Operating Procedures.

**5x5x5** – A national system for recording the evaluation of intelligence.