Lincolnshire Police

Information Assurance Strategy,

Standards and

Working Practices

Author: Richard Burge, Information Manager.

1st July 2018

Contents

Part 1: Information Management Strategy

Part 2: Information Management Standards and Working Practices

Lincolnshire Police

Part 1

Information Management Strategy

Strategy Owner: Chief Constable (Mr Bill Skelly)

Commencement date: 1st April 2009

Review Date: Annually

1. Introduction

1.1 The purpose of this strategy is to set out a strategic direction for further developing our Information Assurance (IA) capability, effectively embedding an IA culture across Lincolnshire Police. This strategy is based upon the National Police Information Assurance Strategy and provides information on the requirements placed on Lincolnshire Police under the National Policing Community Security Policy, including the National Police Information Risk Management Team (NPIRMT) Governance and Information Risk Return (GIRR) and Risk Managed Accreditation Document Sets for police systems. This Strategy supports the implementation of the HMG National Information Assurance Strategy (NIAS) and Information Systems Improvement Strategy (ISIS) programme. Additionally the Management of Police Information (MoPI) Code of Practice (CoP) dictates that the Chief Officer will establish and maintain within their force an Information Assurance Strategy (IAS), under the direction of an officer of ACPO rank or equivalent, complying with guidance and standards to be issued under the Management of Police

Information (MoPI) Code of Practice (CoP) unless that guidance is superseded by regulations made by the Secretary of State under section 53A of the Police Act 1996.

1.2 Policing is an increasingly information-led activity. In order that all organisations working in policing, their partners and the public can have confidence in the information and its secure storage, processing and disposal, it is necessary to have robust IA structures and processes in place. Without these there is a significant and realisable risk of compromise potentially leading to the facilitation of crime, public safety, hindrance to investigations, financial loss, damage to organisational reputation and consequently a reduction in public confidence. This IA strategy reflects the increasing value of information to the Police Service, and the increasingly communal way in which it is used and shared. The intention is for IA to enable police operations and police improvement initiatives. The way that information systems are evolving in the Police Service increases the requirement for Information Risk Management (IRM) and governance, across their delivery, management and use. There is an emphasis on consistency, transparency and ownership of IA Processes, and on measured improvement of those processes.

For clarity, the Home Office definition of Information Assurance is; ***"Information Assurance (IA) is the practice of managing information related risks around the confidentiality, Integrity and availability (CIA) of information, particularly sensitive information. It covers information whilst in storage, processing, use or transit; and the risks created by both malicious and non-malicious actions."***

The Cabinet Office definition of Information Assurance is: ***"…the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users."***

1.3 Lincolnshire Police (hereinafter referred to as the force) has a duty to obtain and use a wide variety of information (including personal information), in order to discharge its responsibilities effectively. This information assurance strategy (IAS) 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 agencies, contractors and partners involved with police information, competently and efficiently carry out their duties. For clarity and as outlined within the 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 arising from common or statute law.

1.4 Subsequent 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 The strategy does not define systems but complements other national initiatives including the development of the Information Systems Strategy for the Police Service (ISS4PS), the National Enabling Programme (NEP), National Law Enforcement Data Service (NLEDS) and National ANPR System (NAS) within which technology and systems are defined.

1.6 The IAS 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 and procedures. By its very nature, the management of all police information will form part of Lincolnshire Police's 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 There being numerous strategic, tactical and operational benefits to the force, which are outlined in Appendix A.

1.8 This strategy does not take a systems approach but will ensure that information is managed across all force objectives, functions and processes.

1.9 The vision sets challenges for the force in respect of data quality. It is the ongoing intention of the force, through the application of the MoPI guidance to improve data quality throughout the relevant business areas. It is furthermore the intention of the force to utilise and align itself where possible with national and local IT improvements in order that the principle of the 'golden nominal' through system/process linkage is attained, thus ensuring that data collected, recorded, evaluated, shared and retained is of the highest quality. The Golden Nominal vision is further enhanced by the introduction of a regional Crime, Case, Custody and Intelligence system (NICHE) for the East Midlands forces (Lincolnshire, Nottinghamshire, Northamptonshire, Leicestershire and Derbyshire) and the City of London.

2. Strategic Aim

Lincolnshire Police vision for Information Assurance is to:

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

2.1 In providing reliable information at the point of need, we will provide the best possible service to our communities and in doing so help realise the force strategic aims.

2.2 IA will be understood by, visible and accessible to all Police Service personnel, and will be embedded in the culture of Lincolnshire Police as well as being aligned across Force/Agency boundaries, particularly when it relates to collaborative working

2.3 Ownership and management of IA issues will be clear to individuals, teams, partners and partnerships, enabling proper consultation with stakeholders prior to IA decisions.

2.4 Information Risk Management framework and processes will be clearly defined, so that individuals have a common understanding of assessment and treatment of risks, which would be conveyable between forces, particularly in the area of force collaboration and aggregated risk management.

2.5 IA standards and procedures are evolved to remain current and relevant to policing objectives and strategies which have a degree of dependency on IA.

2.6 Police information is defined as all information including intelligence and personal data obtained and recorded for a policing purpose as well as personal information obtained in the course of other force business. No differentiation is made in this strategy between information and data and the two terms can be considered synonymous.

3. Strategic Objectives

To achieve its aim, Lincolnshire Police will:

- Work to achieve the required standards to comply with legislation and relevant force policies including the MoPI CoP;
- 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;
- Ensure that the force infrastructure and processes can provide the right information to the right people at the right time for the right purpose;
- Ensure that staff understand the importance of information, the standards necessary, how to use it correctly and how it must be protected from unlawful use.
- Identify and mitigate potential digital obsolescence issues and risk.

3.1 The strategy is designed to ensure that statutory requirements are addressed and that mechanisms are established to ensure that individuals fully understand their responsibilities.

4. Information Assurance Values

To achieve its objectives Lincolnshire Police will be guided by the following values of information management. They reflect the fundamental information management values of the force.

4.1 **The Standards:**

- Is compliant with all relevant legislation, included but not limited to, Data Protection legislation.
- Ensuring best quality of information, right first time.
- The appropriate classification, grading and recording of police information;
- Eradication of unnecessary duplication;
- Evaluation;
- Requirement for information to comply with the principles of the National Intelligence Model (NIM);
- Audit;
- Information Risk management;
- Vetting.
- Accreditation
- IT Security
- Communications Security

4.2 **Business Management:**

- Duty to obtain and manage information;
- Compliance with the National Intelligence Model (NIM);
- Cost-effective information management;
- Commitment to an information culture;
- Information as a business asset – recognising the value of information used in decision-making and program management.

4.3 **People Management**:

- Ownership of information;
- User's responsibilities towards information;
- Competency in handling information;
- Investment in appropriate resources, skills and training.

4.4 **Information Sharing:**

- Duty to share information lawfully;
- Information Sharing as an enabler;
- The right to information for the right person at the right time;
- Protection of sensitive information and sources;
- Obligations of those receiving information.

4.5 **Data/Information Management:**

- Review, retention and disposal of information;
- Conformity/compliance with external requirements;
- Use of appropriate information technology;
- Consider and deal with digital obsolescence issues;
- Security of information;
- Community Security Policy;
- Security Policy Framework;
- Governance and Information Risk Return;
- Police Service Information Assurance Strategy;
- Aggregating data;
- Storage of Information;

- General Data Protection Regulations (EU) 2016/679 (GDPR)
- UK Data Protection Act 2018
- Freedom of Information Act 2000;

5. Benefits

A number of benefits come out of implementing this strategy:

5.1 Enhanced Public and Government confidence in the Police Service's ability to manage and handle information securely.

5.2 Engender greater trust and confidence when sharing information across organisations. Not only will personnel will feel more confident in performing assigned tasks in a secure business environment, third parties and service providers will also feel more secure working for an organisation that places extra emphasis on securing information.

5.3 Better protection reduces the risk of reputational, financial damage or legal liability resulting from compromise of an organisation's information or information systems.

5.4 Detailed review of business processes will enable organisations to be more aware of owned and shared information assets and different types of risks associated to those assets. This will not only provide a deeper understanding of the business processes, but will also identify redundant or duplicated processes, which will reduce bureaucracy, improve performance and reduce operating costs.

5.5 Risk assessment will not only identify critical information assets, but will also identify the types of threat, vulnerability and risks to those assets, so management will be able to mitigate those risks through more cost effective controls.

5.6 Reduced number of security breaches and costs spent investigating them.

5.7 Reduction in adverse publicity and the organisation being better placed to defend its integrity.

5.8 Provide a systematic approach and structure to enable continuous improvement.

5.9 It will enhance the knowledge, awareness and importance of Information assurance and security related issues at all levels within the organisation.

6. Scope of Strategy

6.1 The overarching policy for the police service is embodied in the National Policing Community Security Policy. Therefore a key element of the IA Strategy is to implement the strategic aims of the National Policing CSP, which are:

6.1.1. Enable the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations.

6.1.2. Comply with statutory requirements and meet National Policing expectations of the Police Service to manage information securely.

6.1.3. Help assure Her Majesty's Government that Police Service elements of the Critical National Infrastructure (CNI) are appropriately protected.

6.1.4. Facilitate effective participation with the Transformational Government agenda.

6.2 This strategy also mandates the areas that are identified under MoPI CoP and should be used as good practice for all other information. The MoPI guidance and codes of practice relates to information for a policing purpose as described above. In order to manage our information we have identified all systems that contain such information, splitting them between Designated and Non Designated systems, with strict and well-defined rules in relation to the information held within these respective systems. Please see the Review, Retention and Disposal (RRD) Policy PD54 and the Retention of Police Records (not subject to RRD) Policy PD156.

6.3 It applies to all operational and personal information received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by all staff employed by the force or our strategic partner in the course of carrying out their duties. This document covers all formats of information including electronic, digital and hard copy.

6.4 This strategy does not redefine organisational structures, nor determine technology-based solutions; however, it will inform future technical developments.

7. Strategic Initiatives

7.1 The following Strategic Initiatives will be adopted by the force in order to deliver the Vision statements.

7.1.1 Compliance with the NPIRMT Governance and Information Risk Return (GIRR).

7.1.2 ACPO Council has agreed that the (GIRR) Assessment tool should be the strategic and primary mechanism for establishing compliance against the ACPO/ ACPOS CSP and measuring IA maturity and improvement across the Police Service.

7.1.3 Engagement with GIRR will assist the force in compliance with the Mandatory Requirements of the HMG SPF and IA Standards.

7.1.4 The strategy requires that the force submit a review of GIRR to the National Information Risk Management Team (NPIRMT), in line with the PSN submission to Government Digital Services(GDS).

7.2 Developing Information Risk Management structures in forces and across the wider Police Service.

7.2.1 The police service has an increasingly communal approach to information and therefore there is an increasing degree of aggregated risk. Risk decisions will therefore require consultation of the appropriate risk owners.

7.2.2 Consistency across the police service in the way that information risk is assessed and treated will be facilitated by advice regarding implementation of standards, models (such as the National Police Threat Model) and tools for self-assessment against the GIRR.

7.2.3 The standards and guidance will be clear, consistent and readily available. The information risk management framework will be aligned with that of the corporate risk management framework.

7.3 Developing effective local incident management and recording across the force.

7.3.1 Incident management will be matured within force through the GIRR.

7.3.2 The approach to reporting across the force will be further developed to address incidents which impact on the community, to encompass a wider range of incident reporting, prompt and proper investigation, and the capture of lessons learnt.

7.3.3 Full details of the Force Security Incident reporting procedure can be found within the Force Security Policy PD 55.

7.4 Improve IA Culture.

7.4.1 IA Culture is the way that IA is regarded by individuals within the force. The IA culture needs to be developed to encourage more accountability and ownership of IA risks by individuals; projects and programmes (such that improvements in policing that have any dependencies on IA, consider IA at an early stage).

7.4.2 Individuals will recognise the relevance of IA to them and their own responsibilities. IA will be seen as an enabler rather than a restriction, and as an integral (and not isolated) aspect of police operations and information exploitation.

7.5 Aspire to enhance Information and Risk Management with delivery partners and third parties.

7.5.1 Police need to collaborate and exchange information with other government departments, agencies, and partners (such as Local Authorities, Forensic Science Services, Crime and Disorder Reduction Partners).

7.5.2 An element of trust is required in order to pass information to third parties, which is attained through proven IA measures, including information sharing agreements (ISAs) enforcing the Need to Know, personnel vetting policies, Government Security Classifications and other procedural/technical controls for information exchange.

7.5.3 The GIRR controls are augmented with MOPI, NIM, and legislation such as the General Data Protection Regulations (EU) 2016/679 (GDPR), the UK Data Protection Act 2018 and the Human Rights Act.

7.5.4 The Police risk management frameworks must encompass the communication of risks and risk treatments between police and third parties.

7.6 Ensure policies and processes are clear and consistent, and readily accessible.

7.6.1 HMG IA standards, which are adopted by the Police Service as part of compliance with the Security Policy Framework, are augmented with police-specific standards and guidance (as appropriate).

7.6.2 The approach will ensure that best use can be made of developments in information technology without exposing the force to unnecessary risk.

7.6.3 Where policies, processes and guidance do not address issues that are raised by programmes, the coverage of that guidance should be expanded to meet the demand.

7.6.4 These standards will be developed centrally by NPIRMT and approved via the Information Management and Operational Requirement Coordination Committee (IMORCC) and PIAB.

7.6.5 The standards will be clear and well communicated so that they are accessible and applied consistently.

7.7 IA Capabilities will be defined and improved in support of the strategic initiatives described in this IA strategy.

7.7.1 Some IA Capabilities are made to the police service by the college of policing supporting a community approach to IA. The forces will also develop its own IA Capabilities to support its needs, with at least the minimum roles needed to deliver the required IA Capabilities being implemented.

7.7.2 IA Capabilities across the Police Service will be consistent and in line with HMG/CESG guidance. The individuals who deliver these Capabilities will be appropriately trained, so they are comfortable and competent in making IA decisions and executing their IA responsibilities.

7.7.3 Professionalism in these roles will be enhanced and optimised. The responsibilities associated with the roles should be included in terms and conditions. Job resilience will be established.

8. Responsibilities

8.1 Lincolnshire Police has a corporate responsibility to own and manage all information created, received and held in accordance with the regulatory environment. The person with overall responsibility and ownership of this strategy is the Chief Constable. The Assistant Chief Officer (ACO) has the Community Security Policy (CSP) defined role of

Senior Information Risk Owner (SIRO), although some responsibilities may be delegated to others.

8.2 The force has a corporate responsibility to ensure it has a business continuity plan in place to safeguard its corporate and information assets.

8.3 The person(s) responsible for information assurance in the force will:

i) Ensure that the IAS is available for all staff, partners and the public to view;

ii) 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) Be of the best possible quality

c) Processed under a lawful basis;

d) Shared and disclosed lawfully;

iii) Ensure the integrity of the information.

8.4 All individuals within the force will ensure that all information created, received and held for which they are responsible, is accurate, relevant and kept securely up to date, and that decisions are properly recorded, thereby ensuring accountability with an accurate audit trail.

9. Relationship with Existing Policies

This strategy has been drawn up within the context of:

- Police Service IA Strategy
- MoPI (CoP)
- MoPI Guidance
- MoPI Threshold Standards

- College of Policing authorised professional practice with regard to information management.

and links with other legislation, statute and common law, regulations or national and local policies and procedures affecting the force, see Appendix B.

Please also see Appendix D for policies connected with the Management of Information and therefore this strategy.

10. Relationship with Future Policies

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

N.B: This strategy must be read and implemented in conjunction with force information assurance policies, procedures and processe

Lincolnshire Police

Part 2

Information Management Standards and Working Practices

1. Introduction

1.1 Police information assurance cuts across all police business activities. It is critical that a co-ordinated and cohesive approach is taken to improve police performance in support of the force objectives:

i) Information will be managed to support business processes, whilst remaining specified, explicit and legitimate

ii) Information will be processed fairly, lawfully and in a transparent manner;

ii) Information will be accurate, up-to-date and readily accessible to those who have authority to see it;

iii) Information will be adequate, relevant and limited to what is necessary

iv) Information will be retained only as long as necessary

iv) Information will only be lawfully disclosed or shared where necessary;

v) A consistent approach to managing information will be adopted across the whole force based on the lifecycle of information in accordance with MoPI direction of Review, Retention and Disposal and other Force retention Policies

vi) Methods of information management will be secure, protected, legal, and subject to environmental and proportional cost issues.

1.2 Lincolnshire Police is committed to the following five information management principles as defined by the International Standards Organisation (ISO) 15489:

i) To recognise and understand all types of information;

ii) To understand the legal issues and execute duty of care responsibilities;

iii) To identify and specify business processes and procedures;

iv) To identify enabling technologies to support business processes and procedures;

v) To monitor and audit business processes and procedures.

1.3 These standards provide an opportunity for achieving national consistency through complying with the various National Policies and standards including the community security policy and the MoPI CoP by:

i) Ensuring the force understands the value of information and is able to exploit it as a corporate asset;

ii) Providing the standards for information management in respect of definitions, data standards and the rules for disclosing/sharing;

iii) Integrating all force policies and protocols relating to, and in the context of, managing police information;

iv) 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 Whilst a full list of Information systems is held on the Force Information Asset List (including National systems used by Lincolnshire Police) we have taken the decision to identify all our designated policing purpose and mission critical systems. Each system and business area will have a named business process/system owner of information, known as an Information Asset Owner (IAO) who will be responsible for its creation and accuracy; and act as a custodian of information with their responsibilities being as follows:

i) Completing quarterly information risk assessments on the information they own within their business area.

ii) Provide the S.I.R.O (ACO) via the Force Information Security Officer with annual reports detailing information security use/risk assessments, including access control measures, for each information asset.

iii) Provide an annual information asset list.

iv) Ensure that any action undertaken on their behalf is compliant with all Data Protection Requirements and if not, to ensure that remedial action is taken.

v) Explicitly define and document the access rights granted to date.

vi) Conduct an annual assessment of forth coming changes to service, technology and threat.

Consequently the various business areas and their IAO will be responsible for the various systems as identified below:

Director of Intelligence (Detective Superintendent)

CIS2

NICHE (including Crime, Intelligence, Custody, Warrants, Case Prep and Property)

Pegasus (Formerly PIMMS)
Intelligence E-Pinkies

Crimson (Formerly Crime Manager /Clueso)

Obelisk

ANPR

PINS

Cyccomms

OPS/FCR (Superintendent)

NPIS Command and Control

FCR Contact Management Centre System

Mirage

Airwaves

Innkeeper

Head of Firearms Licensing

NFLMS

FLO

CycFirearms

Head of Crime (Detective Chief Superintendent)

Missing Person-Compact

Video Witness

Custody (Old NSPIS)

Local Policing East (Superintendent)

Sentinel

E-Cins

Head of Professional Standards – (Superintendent)

Crimson (Formerly Crime Manager (ACU))

Complaints and Discipline-Centurion

Vigilance Pro

Supt Tech Futures

PRONTO

DEMS

Information Manager-IMU

Checkmate

Clearcore

GENIE 2

Transearch

Cyc Freedom

Head of ICT – Director of ICT (G4S)

Firewalls

Network

JIRA

Active Directory

LANDesk

Sostenuto

CJS Manager

Acorn

Case Preparation

Clarity

EROS 2

G4S Head of Finance

E-Financials

SAP (Payroll)

T-Police-Finance

I-Trent

Legal Services (Legal Executive)

Amicus-Attorney

Civica

Legal Paper Files

Head of Human Resources (Development) (G4S)

ORIGIN

Crown DMS

T-Police-HR

Staff Personal Files

Head of Occupational Health

Occupational Health Records

1.5 Lincolnshire Police will also process personal and non-personal Information in a variety of other be-spoke and National systems, shared and personal drives all for operational purposes. Each of these will also be owned by an individual or managed by an Information Asset Owner who will be responsible for ensuring the information is processed according to legislation and policy and only retained in accordance with the appropriate Force retention Policies.

1.6 All information within the above be-spoke and National systems, along with those identified as designated or mission critical will be covered by this IAS.

1.7 This IAS will be updated as subsequent systems or relevant business areas have designated or mission critical systems identified or introduced.

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 and all relevant legislation), in order for it to be used for policing purpose. This will enable the force to agree solutions to information management issues locally and nationally.

2.2 Additionally compliance with the ACPO Community Security Policy (CSP) and the advancement of Identity Access Management (IAM) are crucial in the context of information security and MoPI to ensure that access to information is limited to those with authority and when providing an effective audit capability.

2.3 Force policies, procedures and working practices for all key elements of information management will comply with MoPI CoP and other legislative regulations (see Appendix B), with policies and standards affecting the management of information functions across all force business areas.

2.4 Good practice dictates that systems will be integrated and information received or collected will be entered into the system once, on a right first time principal, as part of the operational process at the point of service delivery, without intervening manual processes.

3. Key Focus Areas

Subsequent 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

4. Regulatory Environment

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

5. Strategic and Operational Information Management

The force will address key focus areas as follows:

5.1 <u>Citizen-focused Service Delivery</u>

5.1.1 Lincolnshire Police 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 as citizens are met.

5.1.2 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.

5.1.3 The force will work in partnership with local authorities and other organisations in providing a safer environment for its citizens.

5.2 Governance

5.2.1 The force has a duty to obtain and manage information needed for a policing purpose. The identification of such information and the systems that manage it has been completed, details of the process being outlined in the Force RRD policy PD54. This policy splits such systems into policing purpose and non-policing purpose, with the policing purpose systems split again between Designated and Non-designated. Non-designated systems will only contain policing purpose information that is already held in a Designated system and as such will have very strict retention rules. All information for a policing purpose collected by Lincolnshire Police will be entered into one of the Designated systems, and therefore be subject to force review, retention and disposal rules. All new systems integrated into Lincolnshire Police will be subject to this IAS and its related policies.

5.2.2 All other information obtained and Managed will be processed with due regard to this IA Strategy and retained in accordance with the Retention of Police Records (not subject to RRD) Policy PD 156

5.2.3 The force will manage its information with due regard to the different types of information it is legislatively bound to hold, in particular information that has regulatory constraints upon its publication and that which is for internal use only.

5.2.4 Information will be held where and when it is considered that it is necessary for a policing purpose and assessed for reliability.

5.2.5 Information originally recorded for police purposes will be reviewed in line with MoPI Guidance and be compliant with the principles of all relevant Data Protection Legislation. All such reviews will be documented and require the following to be recorded against them, date of review, reviewers name, outcome and reason for the review, any decision made and the fact the review has been authorised.

5.2.6 When it is reviewed, information originally recorded for policing purposes will be considered for retention or disposal.

- All initial reviews will be conducted at the point of input into a Lincolnshire Police Designated system.
- Any decision as to the retention of information in excess of the guidelines set out under the management of police information will require the completion of the National Retention Assessment Criteria form. These will be completed by the RRD officers and forwarded to their supervisors for approval.
- Disposal of group 1 and 2 information will only take place after a review by the RRD supervisors before disposal within the GENIE application and connected systems.
- Disposal of group 3 information taken out of the time based disposal system will only take place after a review by the RRD supervisor, before disposal from the GENIE application and connected systems.
- Disposal of group 3 and 4 information will be conducted automatically, as per time based disposal and the management of police information guidelines, within the GENIE application and connected systems.
- A proportionate number of reviews will be dip sampled by the Regional RRD manager to ensure compliance to policy and legislation, currently this stands at 5% of those completed.
- All information identified within the Lincolnshire Police Designated systems that can be deleted electronically by the RRD team will be notified via GENIE and Tran search to the records Archive team to ensure the corresponding hard copy information is also appropriately disposed

- Decision as to time-based disposal of group 3 information was originally obtained within Lincolnshire Police via the MoPI project board, any change to these will need the authority of the Chief Constable, or by designated authority via the Information Management Board (IMB).

5.2.7 There will be a need for an inspection of a sample of Force records every 12 months to ensure compliance with the Force RRD policy. The central Audit unit as detailed in the Force Audit Policy and Procedure document will conduct such an Audit.

In order to allow for such audits all items identified for disposal will be subject to disposal schedules, these will be retained within the GENIE application, including time based disposals in group 3, 4 and 5. The initial schedule will include:

- Date of decision.
- Details of the person, object, location or event (POLE) or identification number.
- Details of the information disposed.
- Whether the record was considered inadequate or no longer necessary for a policing purpose.
- Details of the individual authorising the disposal.

These disposal schedules will be retained within the GENIE system for a period of 12 months in order to allow an accurate audit to take place. Such records will be retained solely for that purpose and the details of those P.O.L.E. within them will be limited to that need and will not be made available via any means other than to the auditors and for audit purpose only. At the point of disposal of the information contained within each of the schedules, a further disposal schedule will be created. This will detail the following:

- Date of decision to dispose.
- Number of records.
- Whether the record was considered inadequate or no longer necessary for a policing purpose.

- Details of the individual authorising disposal.

This schedule will contain no personal details and be retained for statistical purposes only and as such will be retained for a period of 10 years.

5.2.8 The Force RRD policy will ensure that all RRD processes are fully adhered to and ensure that police information is relevant to a policing purpose.

5.2.9 Lincolnshire Police 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.

Effective Governance will ensure:

- A corporate approach to information management;
- Delegated responsibilities are defined and understood;
- Good practice is recognised and developed;
- Controls and safeguards exist for integrity and security of police information; and
- Risks are identified and managed.

5.3 Effective and Lawful Use of Information.

5.3.1 The Chief Constable is responsible for ensuring recording procedures are established in accordance with MoPI Guidance to enable information to be as complete and accurate as possible.

5.3.2 The force is committed to continual development of information processes to enable effective information sharing partnerships that ensure disclosure and dissemination in a lawful manner.

5.3.3 The force is committed to providing an environment to support staff in their role of managing the life-cycle of the information.

5.3.4 Where appropriate, the source of the information, 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.

5.3.5The 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.

5.3.6The force must commit to provide the training required by individuals to ensure that relevant data and record quality standards are realised and associated processes are fully understood.

5.4 Information as a Force Asset

5.4.1Each force business area will have a defined IAO and system administrators for systems within that area, who will be responsible for the information life-cycle processes and consistency of those processes across the force.

5.4.2Each designated system will have a system administrator 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.

5.4.3 The force will maintain and develop the quality of facilities and equipment relevant to information provision.

5.5 Information as a Shared Resource

5.5.1The force will ensure information is accurate, reliable and up-to-date, and available to any other police force as specified in MoPI CoP requiring information for police purposes provided that the Chief Constable responsible for the record is satisfied that the police force seeking access to the information applies the principles set out in the MoPI CoP.

5.5.2The force will have in place appropriate protocols and agreements for sharing information as outlined in Force Policy on Information Sharing PD132.

5.5.3 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.

5.5.4 Information Sharing Agreements (ISAs) will be drawn up where a regular exchange of personal information is required, between the police and identified partners.

ISAs are used to formalise arrangements between Lincolnshire Police and identified partners. They identify the types of information to be shared and under what circumstances, the Single Point of Contact (SPoC) for each party and are signed off at an executive level. Within our force ACPO have delegated the executive 'sign off' to Business leads/Departmental Heads.

Once authorised by Business leads/Departmental Heads, ISAs will be published for the benefit of the force on the intranet site, and on the Force Internet site for the benefit of members of the public. The Information Sharing Officer at Force Headquarters will maintain the 'master' library of authorised ISAs.

The identified Police SPoCs will maintain the details of all requests for information, and responses to requests for information in alphabetical order, together with a copy of the ISA. During regular reviews by the partner SPoCs any information contained within the file that has been dealt with and no longer required, will after the required retention period, be permanently destroyed. When not in use, this information will be secured accordingly. All documentation in relation to Information Sharing Agreements will be appropriately marked in accordance with the Government Security Classification (GSC).

One-Off Requests

On occasions there may be the need to share information for a policing purpose with an agency or organisation, where a formal ISA has not been drawn up, and these will be dealt with as a 'One-Off' request.

All 'One-Off' requests will be directed to the Information Sharing Officer (Group-ForceISAOfficer@lincs.pnn.police.uk) who will decide if the request is appropriate, which department the request is to be allocated to provide a response and document the process accordingly. Should such requests need to be made outside of normal office

hours when the Information Sharing Officer is not available and it is necessary for operational reasons of the protection of the public, the information should be shared appropriately. Once completed the details and rationale for the sharing should be forwarded to the Information Sharing Officer as soon as possible.

Should more requests for personal information be made, that meet a policing purpose, then by centralising the One-Off' requests/responses, the need for a formal ISA can be readily identified and drawn up.

5.5.5 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 Constable will require those to whom information is made available to comply with the following obligations:

a) Police information made available in response to such a request will be used only for the purpose for which the request was made;

b) If other information available, at the time or later, to the person or body requesting police information tends to suggest that police information is inaccurate or incomplete, they 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 lead/IAO. The IAO responsible for the police information concerned will then consider, and if necessary, record any additions or changes to the recorded police information.

5.5.6 Information Sharing Agreements will be held centrally and will be subject to review six months after implementation and annually thereafter.

5.6 <u>Infrastructure and Strategic Management of Information.</u>

5.6.1Lincolnshire Police is committed to a consistent approach to the strategic management of information at all levels, led by the relevant Force Information Management Board (IMB).

5.6.2The 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. All such records/documents should be marked (if appropriate) in accordance with the Government Security Classification (GSC). Where current systems do not allow such markings and information from such systems is copied into hard copy form, they should be marked accordingly.

5.6.3 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.

5.6.4 IAO's will be responsible for developing strategic liaisons between departments to facilitate coherent development of information provision.

5.6.5 As Lincolnshire Police 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 in consultation with the Information Technology (IT) Unit and informed by realistic risk assessments. The Force, via the IT department, will also identify and mitigate digital obsolescence risk.

6. Functions and Responsibilities

i) As a matter of policy and procedure, all Lincolnshire Police staff must understand their responsibilities when using or communicating personal or other data and information.

ii) 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.

iii) In addition to individuals' responsibility for information management, there are core levels and functions that have to be identified to ensure that police information is managed effectively, efficiently and lawfully.

6.1 Information Management Board (IMB)

6.1.1 The force will maintain an IMB to implement and monitor the information assurance strategy (IAS) and standards; which will meet quarterly. This board will report directly to

Chief Officer Group (COG) for issues requiring identification or decision to that level, via the Chair.

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;

i) Identification of information assets and the classification into those of value and importance that merit special attention and those that do not;

ii) Quality and quantity of information for effective operation ensuring that, at every level, the information provided is necessary and sufficient, timely, reliable and consistent;

iii) 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;

iv) The protection of information from theft, loss, unauthorised access, improper use, including information which is the property of others;

v) 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;

vi) 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;

vii) Identifying and actioning the appropriateness of a central oversight role for all information held by the force.

6.1.3 The IMB will develop governance structures (including review of the criteria by which the force decides which Group 3 records to review and which to automatically dispose of where the force uses a systems of time-based automatic disposal), policies and procedures to ensure the management of information within the force is undertaken strategically and is aligned with the force objectives.

6.1.4The IMB will oversee the implementation and maintenance of the IAS and standards.

6.1.5The IMB will provide advice to all staff involved in the management of information through the specialisms of its members.

6.1.6The IMB will be responsible for ensuring information assurance training is provided in line with the National Training Strategy and force objectives including:

i) Ensuring a training needs analysis is conducted;

ii) Establishing appropriate training programmes and schedules;

iii) Identifying appropriate training products.

6.1.7Membership of the IMB will comprise of any or all of the following:

a) ACO as Senior Information Risk Owner (S.I.R.O) (Chair);

b) Information Manager (Vice Chair and Force Data Protection Officer)

c) Information Asset Owners from the following business areas:

- Director of Intelligence
- D/Chief Superintendent Head of Crime
- Superintendent OPS/FCR
- Superintendent Local Policing East
- Head of Legal Services/Legal Executive
- Head of Finance
- Head of Human Resources
- Head of Occupational Health
- Head of Firearms
- Supt Tech Futures
- CJS Manager
- Head of Professional Standards

d) Data Protection & FOIA Manager;

e) Regional RRD &Data Quality Manager

f) Force Information Security Officer;

g) Information Technology Security officer (ITSO) and Communication Security Officer (CoMSO)

h) Director Of IT

i) Head of PSD

j) Supt Tech Futures

k) CPT Representative

This list is not exhaustive and can be added to as the need arises.

6.1.8 The Force Risk Register will be utilised to ensure that risks identified in the evolving plans supporting the delivery of the strategy are addressed. Any information risk identified on the Risk Register will be reviewed at each meeting of the IMB.

6.1.9 The IMB will ensure ongoing compliance with the National Policing Community Security Policy (CSP).

6.2 Executive

6.2.1 The Chief Constable has ultimate ownership of the force IAS.

6.2.2 As force Data Controller, the Chief Constable, in line with the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018, 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:

i) Determines why, as well as how, personal data including Special Category data, is to be processed and what security measures will be appropriate;

ii) Has a duty to ensure that the collection and processing of any personal data within the force complies with the data protection principles;

iii) Ensures all actions of the data processor meet those identified under all relevant Data Protection Legislation;

iv) 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. The controls for meeting the force's legal obligations for personal data management can be delegated as appropriate, with clearly defined responsibilities and the ability to report directly to the data controller as necessary.

6.2.4 The Chief Constable has overall executive responsibility for management and use of information within the Lincolnshire Police.

6.3.5 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 Information Manager (IM)

6.3.1 The IM holds responsibility for the management of police information in Lincolnshire Police and as such has responsibility for overseeing all related functions for the management of police information such as data protection, information assurance, freedom of information and disclosure/sharing which may be undertaken by separate internal departments, including agreeing what information can be shared, how and when.

6.3.2 The responsibilities of an IM will include the following:

a) Ensuring:

i) The strategic direction of the force in all information management areas is covered

ii) Force processes and systems adhere to the MoPI CoP, Guidance and Threshold Standards;

iii) A Force Information Assurance Strategy is established and maintained;

iv) All ISA's are held and managed centrally within the force;

v) The process of sharing information is adhered to by both those in a supervisory and user capacity;

vi) Force policies are appropriate to make certain that information is easily accessible and searchable;

vii) The force meets national requirements for the management of the police information;

viii) Compliance with the National Policing Community Security Policy (CSP);

ix) Operating Rules for all force designated systems are available to all staff;

x) Reporting lines exist to allow Business leads/ Department Heads to raise issues to the force information manager or IAO's if necessary;

xi) Reporting lines exist to allow the force information manager to discuss matters (their own or those raised by Business leads /Department Heads) at ACPO level;

xii) Systems and processes are sufficient to effectively co-ordinate all staff roles involved with the management of police information;

xiii) Appropriate role/function is available to represent the force at named forums.

b) Overseeing:

i) The management of all forces information assets and can demonstrate effective linkages between the different functions e.g. IT, Data Protection etc.

ii) Management of freedom of information matters (including compliance with the APP on Information Management);

iii) Compliance with the National Policing Community Security Policy (CSP);

c) Supporting staff to share information appropriately.

6.4 Data Protection Officer

6.4.1 The Data Protection officer will act as the force lead on all Data Protection matters and as such, provide and guidance and act as a single point of contact for Data Protection issues and matters. Specifically they will:

- inform and advise the controller and the employees who carry out their processing of their obligations
- monitor compliance with the Regulation
- provide advice in relation to a data protection impact assessment and to monitor its compliance
- co-operate with a supervisory authority (ICO)
- act as the contact point for the supervisory authority (ICO)

6.5 Senior Information Risk Owner (SIRO)

6.4.1 The appointment at board level of an information risk 'champion' or Senior Information Risk Owner (SIRO) is critical as it sends a clear message to the organisation that the ownership of information risk is considered a strategic responsibility in the same way as financial and legal risks to the business are. The role of the SIRO or IA Champion is to understand how the strategic business goals of the organisation may be affected by failures in the secure use of the organisation's information systems.

a) The SIRO on behalf of the board is responsible for ensuring that:

i) An organisational structure is established for the delivery of effective IA. This should include an effective process for achieving security awareness and accountability;

ii) Funding is available to train staff who have IA responsibilities to meet recognised professional IA standards (CESG Certified Professional (CCP), Institute of Information Security Professional (IISP), Certified Information Systems Security Professional (CISSP) etc);

ii) IA requirements are addressed in strategic planning and are accepted as an integral part of the business;

iv) Corporate security policies (are produced to) ensure consistency across the organisation and compliance with relevant laws, regulations and IA standards;

v) Contingency planning in the form of disaster recovery, business continuity and forensic readiness plans are produced and comply with recognised National and International Standards and good practice guidance;

vi) There is an assurance process to monitor and maintain the effectiveness of the corporate IA policies and plans;

vii) All risk management decisions are justified and accountable in the context of the business requirement and there is a clear understanding of the potential business impact;

viii) An escalation process is established to resolve conflict with or exceptions to corporate IA requirements (business objectives and risk tolerance);

ix) Where an information system crosses organisational boundaries, or connects to a multi-organisational service, controls and reporting mechanisms are in place to support the wider IA governance requirements;

x) Staff with delegated authority are in place to monitor and manage risk and are aware that they are accountable to the board.

6.5 Information Asset Owner (IAO)

a) The SPF requires forces to have Information Asset Owners (IAO) for each identified information asset. IAOs are senior individuals involved in running the relevant business. Their role is to:

i) Lead and foster a culture that values, protects and uses information for the public good;

ii) Know what information assets the Department holds, what enters and leaves the Department and why;

iii) Know who has access and why and ensures their use is monitored;

iv) Understand and address risks to the asset and provides assurance to the SIRO;

v) Ensures the asset is fully used for the public good including responding to requests for access from others.

6.5.1In relation to Review, Retention and Disposal (RRD) of policing purpose information within Lincolnshire Police's designated systems, this will be dealt with in accordance to the RRD Policy PD54 under the control of the Information Manager.

6.5.2The accurate Review, Retention and Disposal of information will ensure the following:

- Safer communities and improved public confidence will follow from more effective tasking and better decision-making. This will be realised by an information management infrastructure containing accurate and complete records that supports effective searching.
- Linked records and elimination of duplicate entries can be expected to deliver tangible operational benefits by:
    1. Less time needed to access better information
    2. Better deployment of operational resources
    3. Associations between crimes and offenders being identified more easily
    4. Reduced risk of missing significant information
- Better access to quality information reduces operational risks, resulting in safer communities and justifies the efforts of all staff in ensuring compliance with MoPI.

6.6 Senior Responsible Owner (SRO)

6.6.1. The SRO is responsible for managing the information risk for specific programmes or projects to ensure they meet the objectives agreed with the SIRO and Board level business owners. The SRO must understand the IA risks to the programme or project and how it may impact the strategic goals of the programme or project. The SRO is also responsible for ensuring that information risk management processes are carried out within the programme or project and cannot assume ownership of any corporate risks that are incurred outside the scope of their particular programme or project. Within Lincolnshire this would normally be the project manager for that specific project.

6.7 Accreditor

a) The role of the Accreditor is to act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting the business requirement and to formally accredit that system on behalf of the SIRO. The Accreditor is also responsible for the following:

i) The Accreditor will need to advise and guide the project or programme team and will play a central role in any committees, panels and groups that are set up to support the project or programme and therefore the accreditation process.

ii) An understanding of IT is useful but the role should not require a deep technical knowledge, more important is an ability to consider information risk management in the round to ensure the physical, personal, procedural and technical controls are balanced. It is important therefore, that the accreditor has access to people who have a professional technical understanding of the technologies involved, to support the accreditation process.

iii) To support this requirement, funding should be identified at the outset for any specialist technical advice and services such as Technical and IA Consultants, IT Health Checks and assurance services.

iv) Accreditors are accountable for their decisions and actions in their role as IA risk assessors and risk managers. They can be called to account for their business actions in a legal proceeding but are not liable in law. This standard supports the need for accountability in the business process and the traceability of risk management decisions.

6.8 Information Technology Security Officer (ITSO)

a) The Information Technology Security Officer (ITSO) is responsible for the security of information in electronic form, including:

i) Developing, implementing and maintaining IT security policy and procedures in accordance with HMG policy and standard;

ii) Developing and promulgating IT security awareness within the organisation;

iii) Representing IT security on internal and interdepartmental security committees;

iv) Providing advice and information on IT security matters to the ISO and SIRO and other stakeholders;

v)Supporting and advising on the accreditation process;

vi) In conjunction with our strategic partner (G4S) ensure that suitable IT security obligations and onward management is reflected in IT service contracts;

vii) Providing a central point of contact on all IT security related issues, both internally and intra-departmentally;

viii) Managing IT security investigations and reporting of IT security incidents to GovCERTUK, Cabinet Office and/or Information Commissioner;

ix)Advising Accreditors, our strategic partner (G4S) and other appropriate stakeholders on any perceived changes in threat, security loopholes, infringements and vulnerabilities that may come to light;

x) Preparing security reports and conducting security surveys required by the Accreditor or SIRO;

xi) Approving any third party connections.

6.9 Communications Security Officer (ComSO)

a) If a Force handles cryptographic material, it must have a designated Communications Security Officer (ComSO). The ComSO is responsible for:

i)Ensuring the Forces compliance with HMG minimum Comsec and Cryptography requirements (including this Standard), including ensuring the Forces compliance is audited annually to ensure compliance with security policy;

ii)Developing, implementing and maintaining organisational communications and cryptographic security policy and procedures in accordance with HMG policy and standards;

iii)Developing and promulgating communications and cryptography security education, training and awareness within the organisation;

iv) Representing communication and cryptography security on internal and interdepartmental security committees;

v) Providing advice and information on communication and cryptography security matters to the SIRO and other stakeholders;

vi) Supporting and advising on the accreditation process for communication systems and those exploiting cryptography;

vii) Ensuring suitable communications and cryptographic security requirements and onward management of these is reflected in relevant services;

viii) Providing a central point of contact on all communication and cryptographic security related issues, both internally and interdepartmentally;

ix) Managing communication and cryptography related security investigations and reporting of incidents in conjunction with the ISO to CINRAS;

x) Providing strategic level communication and cryptography security advice.

xi) Where the ComSO and ITSO roles are separate, they must work closely together, in order to ensure an integrated IA policy within the organisation.

6.10 Core Operational Functions and Responsibilities

The core functions and responsibilities detailed below will ensure that MoPI CoP and Guidance are complied with, however to assist this process the force has set up an Information Management Unit comprising of the following areas of information management:

- Audits
- Information Security
- Information Technology Security
- Staff Vetting
- DBS Disclosures

- Partner Agency Disclosures
- Information Sharing
- Data Protection
- Freedom of Information
- Subject Access
- Force and Regional Review, Retention and Disposal
- Force and Regional Data Quality
- Records Management

6.10.1 <u>All Staff</u>

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

i) To apply the basic principles of effective information management (as contained in MoPI CoP Guidance) including the application of consistent processes and decisions, 'owning' decisions and working as part of a team in a system with many interdependent links;

ii) To recognise the value of trust, confidentiality and information security and the dangers of inappropriate sharing of police information;

iii) To recognise the value of sharing and disclosing information and the dangers of failure to share when the circumstances require it;

iv) To be familiar with, and adhere to, force policy, procedures and processes when managing information;

v) To be aware of the current intelligence requirements; to ensure that information is collected for a policing purpose;

vi) To record information in the appropriate format;

vii) To record information in compliance with the recording and data quality principles, including consistent and accurate recording;

viii) To disseminate information where appropriate;

ix) To apply operating rules relevant to business areas to which they have access;

x) To apply rules relating to information security including applying protective marking to the information being shared under the GSC where applicable or 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;

xi) To only share in accordance with agreed procedures;

xii) To ensure compliance with all relevant legislation including the Human Rights Act 1998, General Data Protection Regulations (EU) 2016/679 (GDPR), the UK Data Protection Act 2018 and Freedom of Information Act 2000.

b) All staff responsible for creating records will:

i) To ensure the persons records are complete;

ii) To quality assure the recording of information, also ensuring the linking together of information where relevant; to identify opportunities for analysis of series or linked events;

iii) Ensure information is evaluated and risk assessed to determine accuracy, value and sensitivity and to determine the necessary action, which could include:

- Immediate response
- Further development
- The need to share
- No action

iv) To apply provenance to the information recorded; to apply relevant priority assessment if appropriate.

c) All staff responsible for reviewing records will:

i) Follow the National Retention Assessment Criteria when reviewing records to determine their continued necessity for a policing purpose, over and above their required retention period.

ii) Document the review process wherever there is no automated mechanism in place: and

iii) Ensure that information to be disposed of is not required for an on-going Policing Purpose.

6.10.2 Force Information Sharing Officer

a) The Force Information Sharing Officer will be responsible for:

i) Quality assuring Information Sharing Agreements (ISAs);

ii) Monitoring compliance with relevant legislation;

iii) Liaising with information owners and other stakeholders in the process;

iv) Liaising with Business Leads/Department Heads when necessary to provide guidance and support on information management;

v) Providing advice and training on good practice;

vi) Identifying officers or police staff able to handle requests that come into the organisation for information sharing;

vii) Ensuring that Information Sharing Agreements are published on the force intranet;

viii) Maintaining a central repository of existing force ISAs;

ix) Reporting on a regular basis to the Data Protection and FOIA Manager;

x) Identifying where there may be need for a force wide approach to sharing requests;

xi) Supporting staff to share information appropriately;

xii) Auditing, on an ad-hoc basis, the decision to share made by users, including the necessity, accuracy and adequacy of information shared;

xiii) Checking whether the decision to share meets a policing purpose or other legal duty or power;

xiv) Ensuring that information being shared does not compromise any police operation or the safety of others;

xv) Ensuring that a risk-assessment process is adhered to by the user when making a decision to share information;

xvi) Ensuring that ISAs are reviewed in accordance with force policy;

xvii) Providing feedback to staff on their performance;

xviii) Ensuring that MoPI Guidance, other relevant ACPO policy and guidance are disseminated and adhered to force-wide.

6.10.3 Records Manager

The force records manager role will be undertaken by the Information Manager who will be responsible for records management as follows:

i) Responsible for retention and management of all Lincolnshire police crime once finalised and received in the Force Central Archives (prior to that the files will be the responsibility of the criminal justice unit);

ii) Responsible for the retention and management of all Lincolnshire Police accident records once finalised and received in the Force Central Archives (prior to this they will be responsibility of the accident records department);

iii) To interrogate force IT systems for information in order to enable case/crime metadata to be recorded alongside nominal records for physical items. (E.g. GENIE, NICHE etc;

iv) Maintain a long-term corporate filing system which supports requests for files or scan-back electronically to all police staff;

v) Keep a register of and maintain accurate records to control the receipt, issue and disposal of any materials;

vi) To respond to Criminal Injuries Compensation Applications;

vii) Maintain and update corporate document and asset management software, using bar coding to track and record physical records;

6.10.4 Data Protection and FOI Manager

a) The DP and FOI managers responsibilities include:

viii) Managing the Chief Officer's statutory obligations in respect of the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018 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;

ix) Maintaining an up to date knowledge of, and advising on, relevant legislation and general developments in data protection matters;

x) Promoting awareness of data protection matters through training, policy development, advice and guidance;

xi) Along with the Force Auditor undertaking systematic auditing and monitoring of information and systems in accordance with the ACPO Data Protection Audit Manual, including risk assessed strategic audit plans;

xii) Ensuring information and systems comply with the relevant legislation including the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018;

xiii) Along with the Force Security Officer 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;

xiv) Investigating and resolving complaints made in relation to the handling of personal information (in relation to data protection);

xv) Assisting where appropriate in the investigation of disciplinary and criminal matters relating to data protection;

xvi) 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);

xvii) Liaising with Business Leads/Department Heads when necessary to provide guidance and support on data protection matters;

xviii) Ensuring that the ACPO Manual of Guidance on Data Protection are disseminated and adhered to force-wide;

xix) Liaise regularly with the Data Protection Supervisor;

xx) Liaising regularly with the Force Information Security Officer and Force Information Technology Officer or equivalent.

b) In relation to freedom of Information the DP and FOI manager must ensure the Data Protection Officer is responsible for:

i) 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;

ii) Maintaining an up to date knowledge of, and advising on relevant legislation and general developments in freedom of information and related matters;

iii) Ensuring that the ACPO Freedom of Information Manual is disseminated and adhered to force-wide;

iv) Promoting awareness of freedom of information matters through training, policy development, advice and guidance;

v) Liaising with BCU Commanders/Department Heads when necessary to provide guidance and support on freedom of information matters;

vi) Liaising on all FOI matters between the force and relevant regional or national bodies (including the ACPO Data Protection and Freedom of Information Portfolio Group).

6.10.5 Force Information Security Officer

a) The force information security officer will be appointed in line with the ACPO/ACPOS Community Security Policy, which specifies the officer's responsibilities including:

i) Acting as the point of contact for all information security issues;

ii) Implementing organisational structures, policies, procedures and risk management programmes with respect to security matters;

iii) Providing advice on the correct and secure operation of information processing systems and applications;

iv) 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;

v) Quality assuring local information security policy documentation;

vi) Demonstrating an approach to implementing security that is consistent with national and local requirements;

vii) Marketing the need for information security;

viii) Providing advise on security education and training;

ix) Co-ordinating all investigative and reporting action that may be undertaken into actual and suspected incidents of security significance;

x) Co-ordinating and advising on the implementation of specific security requirements for new and legacy systems and services;

xi) Establishing and ensuring that thirds party agencies sharing, accessing, storing or processing information and information assets owned by the force, comply with the defined threshold standards;

xii) Maintaining appropriate contacts with other community members, Government departments and regulatory bodies;

xiii) Liaising with Business Leads/Department Heads when necessary to provide guidance and support on information security matters;

xiv) Reporting on a regular basis to the Data Protection & FOIA Manager/Information Manger; representing member interests at a Regional and National level on information security issues;

xv) Ensuring appropriate security measures are afforded to information, including personal data, thereby assisting the forces' compliance with the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018 in order to discharge security responsibilities;

xvi) Liasing on all Information Security matters between the force and relevant regional or national bodies (including the National Police Information Risk Management Team)

6.10.6 Force Information Technology Security Officer

xiv) Acting as the point of contact for all information technology security issues;

xv) Develop security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.

xvi) Provide authoritative advice and guidance on the application and operation of all types of IT security controls including Anti-Virus, Encryption, Email and Internet Content checker.

xvii) Conduct IT security control reviews for a full range of control types and techniques and recommend appropriate action to senior management.

xviii) Providing advice on the correct and secure operation of information processing systems and applications;

xix) 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;

xx) Deliver and develop the development of specialist IS security education and learning for IS and system user management and staff.

xxi) Interpret and apply IT security policies and public standards.

xxii) Demonstrating an approach to implementing security that is consistent with national and local requirements;

xxiii) Marketing the need for technical information security;

xxiv) Conduct investigation, analysis and review following breaches of security control and prepare recommendation for appropriate control improvements.

xxv) Identify threats and provide authoritative advice and guidance on the application and operation of all types of IT Security controls.

xxvi) Co-ordinating and advising on the implementation of specific security requirements for new and legacy systems and services from a technical perspective;

xxvii) Establishing and ensuring that thirds party agencies sharing, accessing, storing or processing information and information assets owned by the force, comply with the defined threshold standards;

xxviii) Maintaining appropriate contacts with other community members, Government departments and regulatory bodies;

xxix) Liaising with Business Leads/Department Heads when necessary to provide guidance and support on technical information security matters;

xxx) Reporting on a regular basis to the Data Protection & FOIA Manager/Information Manager; representing member interests at a Regional and National level on technical information security issues;

xxxi) Ensuring appropriate technical security measures are afforded to information, including personal data, thereby assisting the forces' compliance with the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018 in order to discharge both information and technical security responsibilities;

xxxii) Liasing on all technical information security matters between the force and relevant regional or national bodies (including the National Police Information Risk Management Team)

6.10.7 Force Auditors

i) To undertake a planned audit programme across computer applications and other information systems to determine compliance with the Code of Practice on Information Management, the General Data Protection Regulations (EU) 2016/679 (GDPR), the UK Data Protection Act 2018 and National & in Force audit requirements. To create templates for each new audit programme, ensuring that a corporate approach is adhered to.

ii) To audit, inspect and report on non-compliance of force or Business area activity i.e. wanted files across the force, and to reduce the financial impact to the force by identifying cases and causes of civil claims.

iii) To audit, analyse and report on individual systems to determine compliance with Management of Police Information, National Crime & Recording Systems, National Standard of Incident Reporting, Home Officer Counting Rules, Victims Code, Police National Computer Systems, the General Data Protection Regulations (EU) 2016/679 (GDPR) and the UK Data Protection Act 2018

iv) To audit adherence to local Force instructions, such as dealing with property, financial regulations etc.

v) To liaise with systems owner and relevant staff to collate evidence and undertake the audit work whilst providing advice and guidance relevant to the audits undertaken and enquiries relating to audits. Together with systems owners develop and implement relevant rules and conventions to underpin IT systems ensuring there is a quality audit regime to support them.

vi) Undertake compliance audits to determine if prescribed policies, processes and procedures are being adhered to at all levels. Assist with reviewing and developing the audit processes to ensure fitness for purpose and relevance within the organisation and relevant policies and procedures.

vii) To use the audit methodology to carry out audits and present audit findings, with regard to data quality to stakeholders in a positive, constructive and

logical way that clearly sets out the results obtained and identifies good practice as well as areas where improvements can be achieved.

viii) Perform security audits to eliminate misuse of systems and to ensure that appropriate action is taken to rectify misuse.

ix) Collate relevant information relating to audit findings to enable meaningful comparisons to be made, trends to be identified and analysis to be undertaken and analyse audit information in order to provide valid explanations of audit findings and to reliably inform remedial measures.

x) Prepare hard copy and electronic reports for the Senior Manager Team and operational managers on audit findings within deadlines. Maintain relevant supporting evidence and raw data to support recommendations and findings produced in reports.

6.10.8 Regional RRD & Data Quality Manager

i) Develop, manage and deliver robust policies and procedures to ensure the force complies with the requirements of the Management of Police Information, and force information strategy.

ii) To provide and advise senior management on Data Quality and RRD procedures, also being responsible for ensuring service level agreement targets are achieved.

iii) To manage the resolution of disputes arising from recommendations or decisions made concerning the retention and disposal of police records.

iv) Actively promotes records management as a corporate function and ensures alignment to wider management of information throughout the force e.g. structured file management system.

v) Represents the region at national and local level in matters relating to RRD and Data Quality issues.

vi) To co-ordinate and harmonise the force approach to the management of police information, knowledge repositories, and in particular, to meet MoPI data quality principles and promote good records management practice.

vii) To maintain regular liaison with business and system owners to ensure that the necessary links are in place which support and develop the concept of the "Golden Nominal".

6.10.9 DBS Disclosure Manager

i) Develop, manage and deliver robust policies and procedures to ensure the force complies with the requirements of the Management of Police Information, disclosure, and force information strategy.

ii) To provide and advise senior management on disclosure information and to ensure disclosures have been properly evaluated before disclosure to DBS. Also responsible for ensuring service level agreement targets are achieved.

iii) To ensure all disclosures have been fully 'Risk Assessed' in accordance with the DBS Quality Assurance Framework (QAF). To manage the information extraction, disclosure decisions and text for Chief Officer delegate signature, as well as ensuring a percentage check is made with regard non-disclosure decisions made by the Disclosure Unit Officers.

vi) Represents the Force at national and local level in matters relating to DBS Disclosures.

iv) To co-ordinate and harmonise the force approach to the management of police information and all DBS disclosure issues.

6.10.10 Business Lead/Department Manager

a) The responsibilities of a Business Lead or Department Manager, with regards to information management include:

i) Ensuring the Business area or department under their command complies with all force policies, procedures and processes relevant to information management;

ii) Ensuring the Business area or department under their command complies with all legislation relevant to information management;

iii) Ensuring the Business area or department under their command complies with the MoPI CoP, Guidance and Threshold Standards;

VI) Liaising with the Force information, RRD and Data Quality Manager, DBS Disclosure manager, Data Protection and FOI Manager, Force Data Protection Officer, Force Freedom of Information Officer, Force Information Security Officer or Force Information Technology Officer where necessary to seek advise and ensure information is shared appropriately within the boundaries of force and national policy and legal framework.

iv) Raising issues on information management to the Regional RRD and Data Quality Manager, Force Data Protection and FOI Manager, Force Information Security Officer or Force Senior Vetting Officer who may then liaise with the IM or equivalent (where necessary);

v) Ensuring data quality is treated as a priority;

vi) Ensuring staff are recording information on the appropriate format;

vii) Ensuring staff responsible for recording, and undertaking reviews of police information are trained in accordance with the MoPI National Training and Delivery Strategy.

6.11.11 Senior Vetting Officer

a) A Senior Vetting Officers responsibilities include:

i) Ensuring that all Police Officers, Police and Partnership staff, Contractors and Partner Agencies are vetted to the appropriate level for their roles in accordance with National and Force Vetting Policy, Vetting Code of Practice and the APP on Vetting.

ii) Ensuring effective decision making in respect of granting, refusing or withdrawing Force or National Security Vetting clearance.

iii) Liaising with the Force Security Officer, Force Information Technology Officer, Data Protection Officer and the Professional Standards Department for vetting matters.

vi) Ensuring Aftercare and Renewals are carried out to continue the integrity of the individual working for and with Lincolnshire Police.

v) Maintain appropriate contacts with other Forces and Agencies to ensure best practice and achieving a collaborative working approach to vetting processes and procedures.

vi) Liaising with Business Leads/Department Heads when necessary to provide guidance and support on vetting matters.

7. Audit and Compliance

7.1 The force, in the form of the Data Protection and Freedom of Information Manager, RRD and Data Quality Manager, DBS Manager, Force Information Security Officer and IT Security Officer, 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 co-ordination takes place and includes:

i) Ensuring that information management policies and procedures are being communicated to appropriate force personnel and are being adhered to;

ii) Monitoring use of shared/personal storage space;

iii) Ensuring that metadata exists for all documents and files;

iv) Monitoring the use of the force file management systems and processes, including appropriate naming and assigning of metadata for all documents and folders;

v) Ensuring that appropriate data standards and targets are in place and met;

vi) Ensuring that appropriate paper filing takes place;

vii) Ensuring that the accuracy of data is regularly assessed.

viii) Ensuring that information is only held for as long as is necessary and disposed securely.

7.2 The force in the form of the Force Auditor, will have responsibility for ensuring regular information quality assurance audits across business areas. This will include:

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

ii) Setting compliance criteria;

iii) 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.

Appendix A

BUSINESS BENEFITS		
Strategic Benefits	**Tactical Benefits**	**Operational Benefits**
1. IMPROVED POLICE PERFORMANCE	1.1 Nationally consistent and effective management of information 1.2 Improved auditing of decision-making process 1.3 Increased understanding of and compliance with relevant legislation 1.4 Reduced civil actions and complaints against forces as a result of poor information management	1.5 Improved data quality 1.6 Responsibilities in relation to information management are clear 1.7 Less officer/staff time and effort is needed to access information 1.8 Less impact of civil action and formal complaints on officer/staff time and wellbeing
2. SAFER COMMUNITIES	2.1 More informed decision making 2.2 Improved targeting 2.3 Improved processes for joint agency working 2.4 Effective management of high risk offenders 2.5 Enhanced disclosures processes 2.6 Improved protection of children and vulnerable adults	2.7 Related information is linked and associations between crime and offenders are more easily made 2.8 Better deployment of operational resources 2.9 Increased willingness of partner agencies to share information 2.10 Less bureaucratic processes for sharing information
3. INCREASED	3.1 Improved victim/witness satisfaction	3.4 Increased reporting of crime

PUBLIC CONFIDENCE	3.2 Improved community relations 3.3 Improved public confidence in the information we hold	3.5 Increased provision of community intelligence 3.6 Increased corporate knowledge provides better service to all areas of the community

Appendix B

Regulatory Environment

- Police Act 1997 (Act V)
- Freedom of Information Act 2000
- Criminal Justice Act 2003
- Crime and Disorder Act 1998
- Serious & Organised Crime & Police Act 2005
- Sexual Offenders Act 2004
- Limitation Act 1980
- Criminal Procedures & Investigations Act 1996
- General Data Protection Regulations (EU) 2016/679 (GDPR)
- UK Data Protection Act 2018
- Children Act 1998
- Children Act 2004
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Domestic Violence, Crime and Victims Act 2004
- Protection of Freedoms Act 2012
- Code of Practice on the Management of Police Information (2005)
- APP on Information Management
- Code of Practice on the NIM (2005)
- National Policing Community Security Policy

- Governance and Information Risk Return
- Security Policy Framework
- Information Assurance Standards
- APP on Investigation and Public Protection
- Manual of Guidance on the NIM (2005)
- NIM Briefing Model
- CPS Disclosure Manual
- ACPO Guidance for the investigation of corruption in the police service (2003)
- Retention Guidelines for Nominal Records
- Home Office Circular 25/2003
- Home Office Circular 45/1986
- Home Office Circular 05/2005
- Mis-use of Computer Act 1990

Appendix C

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 the General Data Protection Regulations (EU) 2016/679 (GDPR) or the UK Data Protection Act 2018, or 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 therefore 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, cataloguing/identification, storage and preservation of, and access to, information.
Information Management	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 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	The field of management responsible for the efficient, and systematic control of the creation, receipt, maintenance, use and disposition of records. This includes processes for capturing and

maintaining evidence of, and information about, business activities and transactions in the form of records. (ISO 15489:2001)

Appendix D

Index of Information Management Sub-Policies

The following force policies with relevant standards, protocols and agreements are not stand-alone nor should they be adhered to in isolation but sit beneath an over-arching force Information Management Strategy and standards as statements of intent and procedures for not only achieving and maintaining good management of police information but also for reaping the business benefits that are the outcome of this good practice. The policies listed below are not an exhaustive list and can and should be added to as the need arises.

1. Data Protection & FOIA Policy

Policy number/reference: PD 141

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: Force Information Security Policy (FISP)

ACPO/ACPOS CSP

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Record of Processing Activities

Force Privacy Notice

Information Management Strategy

Review Retention and Disposal (RRD) Policy

Retention of Police Records (not subject of RRD) Policy

Mis-use of Computer Act 1990

Freedom of Information Act (FOIA) 2000

Management of Police Information (MoPI) Manual of Guidance 2010

MoPI CoP 2005

2. Data Quality and Data Cleansing Policy

Policy number/reference: PD 120

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI CoP 2005

MoPI Manual of Guidance 2010

Information Management Strategy

Information Management Policy

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

APP Information Management

RRD Policy

3. E-Mail Archive and Retention

Policy number/reference: PD 146

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Policy

MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

Retention of Police Records (not subject to RRD) Policy

ACPO/ACPOS CSP

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

MoPI CoP 2005

4. Force Security Policy

Policy number/reference: PD 55

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: ACPO/ACPOS Community Security Policy (CSP)

Force Information Security Policy (FISP)

Information Management Strategy

Manual of Protective Security (MoPS)

HMG Information Security Standards

ISO/17799

BS 7799

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

Data Protection and FOIA Policy

MoPI Manual of Guidance 2010

MoPI CoP 2005

5. Forensic Readiness Policy

Policy number/reference: PD 188

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: ACPO/ACPOS Community Security Policy (CSP)

Force Information Security Policy (FISP)

Manual of Protective Security (MoPS)

HMG Information Security Standards

ISO/17799

BS 7799

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

6. Regional Government Security Classification Policy

Policy number/reference: PD 224

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Policy

Data Quality Policy

Information Management Strategy

ACPO/ACPOS CSP

MoPI Manual of Guidance 2010

MoPI CoP 2005

Government Protective Marking Scheme (GPMS)

7. Information Audit and Procedures Policy

Policy number/reference: PD 135

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Data Protection and FOIA Policy

RRD Policy

Mis-use of Computer Act 1990

ACPO Data Protection Audit Manual

MoPI Manual of Guidance 2010

MoPI CoP 2005

Information Management Strategy

Force Information Security Policy (FISP)

ACPO/ACPOS CSP

8. Information Sharing, Disclosure and Dissemination

Policy number/reference: PD 132

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Manual of Guidance 2010

MoPI CoP 2005

Force Information Sharing Policy and Information Sharing Protocols/Agreements

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Information Management Strategy

Data Protection and FOIA Policy

APP Information Management

Freedom OF information Act 2000 (FoIA 2000)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

CPS Disclosure Manual

ECHR Directive

9. Management of Police Information Policy

Policy number/reference: PD 118

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: Information Management Strategy

Domestic Violence Policy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

RRD Policy

Child Protection Policy

Intelligence Policy

Custody Policy

Firearms Policy

Crime & Detection Policy

MoPI Manual of Guidance 2010

MoPI CoP 2005

10. Partner Agency Disclosure Policy

Policy number/reference: PD 134

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Manual of Guidance 2010

MoPI Policy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Data Protection and FOIA Policy

Information Management Strategy

ACPO/ACPOS CSP

MoPI CoP 2005

11. Common Law Police Disclosures to Employers

Policy number/reference: PD 199

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Information Management Strategy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Data Protection and FOIA Policy

MoPI CoP 2005

MoPI Policy

12. PND Audit Policy

Policy number/reference: PD 179

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: ACPO/ACPOS Community Security Policy (CSP)

Force Information Security Policy (FISP)

Manual of Protective Security (MoPS)

HMG Information Security Standards

ISO/17799

BS 7799

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

MoPI Manual of Guidance 2010

MoPI CoP 2005

MoPI Policy

Force Information Security Policy (FISP)

PND Policy

13. Privacy Impact Assessment (PIA) Policy

Policy number/reference: PD 170

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Policy

MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

ACPO/ACPOS CSP

NIM Manual of Guidance

Al Force Policies and Procedures

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

14. Protecting Data Stored on Portable Media

Policy number/reference: PD 139

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: ACPO/ACPOS Community Security Policy (CSP)

Force Information Security Policy (FISP)

Manual of Protective Security (MoPS)

HMG Information Security Standards

ISO/17799

BS 7799

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

MoPI Manual of Guidance 2010

MoPI CoP 2005

MoPI Policy

15. Records Management Policy

Policy number/reference: PD 191

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Policy

MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

Information Management Strategy

ACPO/ACPOS CSP

NIM Manual of Guidance

Force Audit Policy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

MoPI CoP 2005

RRD Policy

16. Remote Access Operating Policy

Policy number/reference: PD 147

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Policy

MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

ACPO/ACPOS CSP

NIM Manual of Guidance

Force Audit Policy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Information Management Strategy

MoPI CoP 2005

17. Retention of Police Records (not subject of RRD) Policy

Policy number/reference: PD 156

Owner of policy: Information Manager

Review schedule: Annual

Location: IMU/Intranet

Linkage with: MoPI Policy

MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

Information Management Strategy

ACPO/ACPOS CSP

NIM Manual of Guidance

RRD Policy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

MoPI CoP 2005

18. Review, Retention and Disposal

Policy number/reference: PD 54

Owner of policy: Information Manager

Review schedule: Annual (October)

Location: Planning and Policy Department/Intranet

Linkage with: MoPI Manual of Guidance 2010

Force Information Security Policy (FISP)

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

ACPO/ACPOS CSP

NIM Manual of Guidance

Force Audit Policy

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Information Management Strategy

MoPI CoP 2005

MoPI Policy

Notifiable Occupations Policy

Missing Persons Policy

19. Risk Management

Policy number/reference: PD 122

Owner of policy: Head of Strategic Development

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: Force Information Security Policy (FISP)

Force Flagging Policy

Force SyOpS

Force Compliance Policy

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

General Data Protection Regulations (EU) 2016/679 (GDPR)

UK Data Protection Act 2018

Information Management Strategy

FoIA 2000

Health and Safety Policy PD27 (1)

Annual Policing Plan

Lincolnshire Police Strategic Plan

Health and Safety Strategy Plan

20. Staff Vetting

Policy number/reference: PD 130

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: National Intelligence Model (NIM)

College of Policing Vetting COP

APP Vetting

Government Protective Marking Scheme (GPMS)

Government Security Classification (GSC)

Information Management Strategy

MoPI Manual of Guidance 2010

ACPO/ACPOS CSP

21. Management of Cryptographic Systems Policy

Policy number/reference: PD 208

Owner of policy: Information Manager

Review schedule: Annual

Location: Planning and Policy Department/Intranet

Linkage with: Security Policy

ISO 17799

BS7799

HMG IS4