



Policy Directive

INFORMATION MANAGEMENT POLICY

Policy Identification Number	01/15
Protective Marking	NOT PROTECTIVELY MARKED
Policy Ownership:	Assistant Chief Constable
Department	Operational Support
Branch	Information Security Unit
Author	Head of Information Security and Records Management
Policy Approved By:	Assistant Chief Constable
Service Executive	
Department or Branch Head	Operational Support
Date Of Approval	18 March 2010
Date First Issued:	9 December 2015
Version Number	1
This Version Issued:	9 December 2015
Review Date:	2 years from issue date

2. POLICY STATEMENTS

(1) **This Information Management Policy is designed, as an overarching document to encompass the information requirements of the Police Service of Northern Ireland (PSNI) in the following business areas:-**

- (a) Information Security;
- (b) Records Management;
- (c) Quality Police Information (QPI) incorporating the Management of Police Information (MoPI);
- (d) Freedom of Information/Data Protection;
- (e) Information and Communications (ICS) IT Strategy;
- (f) Vetting Disclosure;
- (g) Quality Assurance/Quality Audit Programme; and
- (h) Intelligence

(2) **Scope**

- (a) The Information Management Policy embraces all information held by the PSNI whether termed police information or otherwise. Five policing purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining of police information (S32 – Police (NI) Act 2000).
- (b) Police information is information required for a policing purpose and necessary for:-
 - (i) Protecting life and property;
 - (ii) Preserving order;
 - (iii) Preventing the commission of offences;
 - (iv) Bringing offenders to justice; and
 - (v) Any duty or responsibility arising from common law or statute law.
- (c) Administrative records relate to non-policing information that are essential to the day-to-day business and administration of the PSNI.

3. INTRODUCTION

(1) **Executive Summary**

- (a) Data quality is fundamental to successful information management. It is essential that information is recorded accurately from the outset. All information should conform to the data quality principles of accuracy, adequacy, relevance, and timeliness. It must be accessible and understandable to enable police officers and police staff to carry out their duties.
- (b) Information will be managed in a secure fashion, ensuring continuity and minimising the impact of security threats or incidents. PSNI will ensure that a review, retention and disposal schedule is implemented for both electronic and paper records.
- (c) Shared information will be lawful and properly controlled (both inside and outside the police service). The PSNI will meet its responsibilities by managing information consistent with our legal and ethical obligations. Information will be managed within PSNI's Governance Structure and Assurance Framework.

(2) Aims and Objectives

- (a) The strategic aims of the Information Management Policy are to:-
- (i) Comply with Government standards, advice and guidance and take account of national developments while setting standards in compliance with relevant legislation;
 - (ii) Assist the discharge of PSNI's general policing functions while creating the basis to supporting information sharing with other police services and our partner agencies;
 - (iii) Assist the development of effective records management for police information; and
 - (iv) Improve police performance by ensuring information is reliable, accessible and available at the point of need.
- (b) To achieve these aims, the policy objectives are to:-
- (i) Create and maintain relevant policies, procedures and guidance;
 - (ii) Provide the overarching strategy governing PSNI's QPI;
 - (iii) Develop PSNI Records Review Retention and Disposal schedule;
 - (iv) Reduce the number of information 'silos' by ensuring records are linked and in a format which is searchable;
 - (v) Create and store records electronically whenever possible; and
 - (vi) Develop appropriate storage systems.

(3) Application

This Policy does not stand-alone; it is intrinsic to how the PSNI manages all information and as such both informs and is informed by, all other PSNI Policies and Service Procedures.

(4) Legal Basis

The following legislation imposes the need for effective management of all PSNI records, both paper and electronic:-

- (a) It is a legislative requirement to implement records management under the terms of the Public Records Act (NI) 1923 and the Disposal of Records Order (S.R. & O. 1925 No. 167);
- (b) Public Authorities are obliged to comply with the Freedom of Information Act 2000 (FOIA) and the associated Lord Chancellor's Code of Practice on the discharge of functions under the Freedom of Information Act (s.45) and Records Management (s.46);
- (c) Environmental Information Regulations 2004;
- (d) The Data Protection Act 1998 (DPA);
- (e) Human Rights Act 1998;
- (f) Criminal Procedure and Investigations Act 1996; and
- (g) There is no legal requirement for the introduction of QPI to PSNI. However, there are statutory obligations and guidance relevant to the area of police information and data. References for these documents can be found at Appendix 'A'.
- (h) Regulation of Investigatory Powers Act 2000.

4. IMPLICATIONS OF THE POLICY

(1) Financial Implications/Best Value/Continuous Improvement/Efficiency

The Policy sets out guidance to:-

- (a) Improve public protection;
- (b) Improve internal information policies; and
- (c) Improve information sharing.

(2) Human Resources/Training

All police officers and nominated police staff will be appropriately trained in the key issues and principles of QPI through an e-learning programme.

(3) Partnerships

New policies and procedures will be used to ensure that information shared with other agencies meets the standards set out in Information Sharing Agreements (ISAs).

(4) Risks

Failure to meet legislative and statutory obligations may lead to:-

- (a) Reduced level of public protection; Art. 2 risks to sources of police information;
- (b) Loss of public confidence;
- (c) Criticism from HMI/CJINI/PONI/OSC;
- (d) Failing to meet PSNI QPI standards;
- (e) Inadequate governance structures;
- (f) Inappropriate and outdated information management systems and processes;
- (g) Inability of the Chief Constable and Assistant Chief Constable (ACC), Operational Support to discharge their functions within the Information Management Policy Document.
- (h) Adverse rulings by the Information Commissioner's Office including potential enforcement action.
- (i) Major long-term impairment in our ability to investigate serious organised crime.

(5) **PSNI Policy**

The implications of QPI must be considered when any PSNI Policy dealing with police information is being formulated. The Policy audit tool will be used for this purpose and has been amended accordingly.

(6) **Project Management**

Project Boards and Project Managers will ensure that their reporting mechanisms take due account of the implications of this Policy.

(7) **Estates**

Not applicable.

(8) **Consultation**

(a) **Previous External Consultation**

- (i) NPIA now College of Policing;
- (ii) North West Region Policing Forum;
- (iii) Avon and Somerset Constabulary; and
- (iv) The Association of Chief Police Officers in Scotland (ACPOS) now NPCC.

(b) **Previous Internal Consultation:**

- (i) All Chief Officers;
- (ii) Head of Corporate Development;
- (iii) PSD now S5;
- (iv) Head of Firearms Branch;
- (v) Criminal Justice, Crime Operations and Human Resources (HR) Departments; and
- (vi) District Commanders.

(c) **Current Internal Consultation**

- (i) ISU;
- (ii) RMU;
- (iii) Head of FOI & DP;
- (iv) Vetting Disclosure;
- (v) C3 Intelligence.

5. HUMAN RIGHTS/EQUALITY/CODE OF ETHICS/FREEDOM OF INFORMATION

- (1) This policy is deemed to be Human Rights compliant; it has been screened for Section 75 considerations and meets integrity standards. It is suitable for disclosure in accordance with the Freedom of Information Act (FOIA) 2000.
- (2) Police officers are reminded of their obligations under Articles 3 and 8 of the PSNI Code of Ethics. Police staff are reminded of their obligations under the Northern Ireland Civil Service (NICS) Code of Ethics.

6. REVIEW

The Head of Information Security & Records Management and the Head of Data Protection/Freedom of Information are responsible for reviewing the contents of this Policy every two years.

7. CANCELLATION

Policy Directive 03/10 ' Information Management Strategy ', is hereby cancelled.