



NOT PROTECTIVELY MARKED

WEST MIDLANDS POLICE

Force Policy Document

POLICY TITLE:	Information Management Policy
POLICY REFERENCE NO:	Inf/01

Executive Summary.

West Midlands Police (referred to as 'the force' thereafter) with immediate effect introduces a new Information and Records Management Policy (previously known as Records Management Policy) in line with The Management of Police Information 2010 (MoPI) Code of Practice (CoP) and Guidance. This policy should be read and implemented in conjunction with the Data Protection Act 1998 (DPA), the WMP force retention schedule and MoPI composite offence lists for groups 1, 2 and 3. These documents are located on the MoPI website.

**Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.

Intended Policy Audience.

West Midlands Police Officers, Staff, PCSOs and Special Constables

Current Version And Effective Date.	Version 1.2	August 2014
Business Area Owner	Intelligence	
Department Responsible	Information Management	
Policy Contact	Kate Jeffries, Head of Information Management	
Policy Author	Charlotte Capener	
Approved By	ACC Forsyth	
Policy Initial Implementation Date	01/11/2011	
Review Date	20/08/2015	
Protective Marking	Not Protectively Marked	
Suitable For Publication – Freedom Of Information	Yes	

Supporting Documents

- *Data Protection Act 1998 (DPA)*
- *The Management of Police Information 2010 (MoPI) Code of Practice (CoP) and Guidance*
- *WMP force retention schedule*
- *MoPI composite offence lists for groups 1,2 and 3*

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.

PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Diversity Vision Statement and Values

“Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values”

“All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay.”

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1.	INTRODUCTION.....	5
2.	SCOPE AND DEFINITIONS.....	5
3.	AIMS OF INFORMATION MANAGEMENT POLICY.....	6
4.	ROLES AND RESPONSIBILITES.....	7
5.	LEGAL AND PROFESSIONAL OBLIGATIONS.	8
6.	INFORMATION ASSET REGISTER.....	8
7.	RETENTION AND DISPOSAL SCHEDULES.	8
8.	RECORDS MANAGEMENT SYSTEMS AUDIT.	9
9.	EQUALITY IMPACT ASSESSMENT (EQIA).....	9
10.	HUMAN RIGHTS.....	9
11.	FREEDOM OF INFORMATION (FOI).....	10
12.	TRAINING.	10
13.	PROMOTION / DISTRIBUTION & MARKETING.....	10
14.	REVIEW.	10
15.	VERSION HISTORY.....	11

1. INTRODUCTION.

- 1.1 Information & Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.
- 1.2 West Midlands Police pays due regard to the Management of Police Information (MoPI) guidance as published by the Home Office. It is based on current requirements and professional best practice.
- 1.3 The force's records are its corporate memory, providing intelligence, evidence, a history of actions and decisions and represent a vital asset to support daily functions and operations. Creation and adoption of this policy protects the interests of the force and the rights of its staff and members of the public. It supports consistency, continuity, efficiency and productivity.
- 1.4 The Command Team has adopted this information management policy and is committed to ongoing improvement of its information management functions as it believes that it will gain a number of organisational benefits from so doing. These include:
- better use of physical and server space;
 - better use of staff time;
 - improved control of valuable information resources;
 - compliance with legislation and standards; and
 - reduced costs.
- 1.5 The force also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of information management as a designated corporate function.
- 1.6 This document sets out a framework within which the staff responsible for managing the force's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.
- 1.7 This policy document should be read in conjunction with the further detail provided on the force intranet records management web pages.

2. SCOPE AND DEFINITIONS.

- 2.1 This policy relates to all information held in any format by the force. These include:
- all corporate records required to support policing purpose (e.g. HR, property, financial & accounting records, and notes associated with complaints); and
 - all operational records.

NOT PROTECTIVELY MARKED

2.2 **Records Management** is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational and business needs of the force and preserving an appropriate historical record. The key components of information & records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- review;
- archiving; and
- disposal.

2.3 The term **Records Life Cycle** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

2.4 In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the force in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

2.5 **Information** is a corporate asset and is essential in the effective prevention and detection of crime. The force's records are important sources of administrative, evidential and historical information. They are vital to the force to support its current and future operations (including meeting the requirements of Data Protection, CPIA & Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

3. AIMS OF INFORMATION MANAGEMENT POLICY.

3.1 The aims of our Information Management Policy are to ensure that:

- **Information is available when needed** - from which the force is able to detect and prevent crime;
- **Information can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **Information can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **Information can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;

NOT PROTECTIVELY MARKED

- **Information is secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

4. ROLES AND RESPONSIBILITIES.

Chief Constable:

4.1 The Chief Constable has overall responsibility for records management in the force. As accountable officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

4.2 The force has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Senior Information Risk Owner (SIRO):

4.3 The SIRO is responsible for the overall delivery of the Information Management Policy through the Strategic Information Management Board (SIMB) which directs the activities of the Information Assurance Bronze group.

Caldicott Guardian:

4.4 The force's Caldicott Guardian has a particular responsibility for reflecting the interests of all staff regarding the use of health records that contain personal identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Head of Information Management:

4.5 The Head of Information Management is responsible for ensuring that this policy is implemented through the Information Management Teams and that the records management system and processes are developed, co-ordinated and monitored.

Information Asset Owners (IAO):

4.6 The responsibility for information management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units and business functions within the force have overall responsibility for the management of records generated by or used in their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the force's records management policies.

Supervisory Staff:

- 4.7 All supervisory staff have a responsibility to ensure the accuracy of the information that their staff enter into force systems.

All Staff:

- 4.8 All staff, whether permanent or contract, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they enter data that is accurate and proportionate, in keeping with this policy and with any guidance subsequently produced.

5. LEGAL AND PROFESSIONAL OBLIGATIONS.

- 5.1 The force will take actions as necessary to comply with the legal and professional obligations set out in national guidance and legislation, in particular:

- Management of Police Information 2010;
- The Data Protection Act 1998; and
- The Freedom of Information Act 2000;
- Criminal Procedure and Investigations Act 1996

and any new legislation affecting records management as it arises.

6. INFORMATION ASSET REGISTER.

- 6.1 The force will maintain an Information Asset Register through which departments and other units (via the IAO) can register the records they are maintaining. The inventory of record collections will facilitate:

- the classification of records into series; and
- the recording of the responsibility of individuals creating records.

- 6.2 The register will be reviewed annually at the SIMB.

7. RETENTION AND DISPOSAL SCHEDULES.

- 7.1 It is a fundamental requirement that all of the force's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the force's business functions.

- 7.2 The force has published its WMP retention schedule which can be found in the Information Management web pages. The WMP retention schedule will be reviewed annually.

8. RECORDS MANAGEMENT SYSTEMS AUDIT.

8.1 The force will regularly audit its records management practices for compliance with this framework.

8.2 The audit will:

- Identify areas of operation that are covered by the force's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures

8.3 The results of audits will be reported to the SIMB.

9. EQUALITY IMPACT ASSESSMENT (EQIA).

9.1 The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how WMP has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

10. HUMAN RIGHTS.

10.1 This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

11. FREEDOM OF INFORMATION (FOI).

- 11.1 Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 1 of this policy has been GPMS marked as Not Protectively Marked.
- 11.2 Public disclosure does not automatically apply to supporting Force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number

12. TRAINING.

- 12.1 All force staff permanent and contract, will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes, guidance and policies.

13. PROMOTION / DISTRIBUTION & MARKETING.

- 13.1 The following methods will be adopted to ensure full knowledge of the Policy:
 - Message of The Day
 - Policy uploaded onto the Force Intranet EQUIP Portal
 - Information on Information Management Intranet pages

14. REVIEW.

- 14.1 The policy business owner Intelligence (Information Management) maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.
- 14.2 The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.
- 14.3 A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted by the date shown as indicated on the first page.
- 14.4 Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.
- 14.5 Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

Ch S

CHIEF CONSTABLE

15. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
IM/RM v1	June 2014	Review and subsequent removal of previous RM policy. Replaced in its entirety by the Information Management Policy. The previous policy to form the basis for a process/procedure document.	KJ/CC
IM v1.01	July 2104	Addition of further legislative guidance.	CC/KJ
V1.1	27/08/2014	Added code of ethics section, CC signature, approval details	Vicki Couchman 56408
V1.2	29/8/14	Changed SIIMB to SIMB	Kate Jeffries 50061