



RECORDS MANAGEMENT

Executive Summary

As a public body WMP are required by law to manage our information appropriately and in accordance with legislation and guidance.

Records Management (RM) is the processes and controls by which an organisation manages all aspects of records whether internally or externally generated, corporate or operational and in any format, hardcopy or electronic from their creation all the way through their lifecycle to their eventual disposal or preservation.

By placing such controls around the lifecycle of a record, we can ensure our information demonstrates the key attributes of authenticity, reliability, integrity and accessibility. This policy also supports consistency, continuity, efficiency and productivity.

The Force's records and information are its corporate memory, providing intelligence, evidence, a history of actions, decisions and represent a vital asset to support daily functions and operations.

Authorised Professional Practice (APP):

- This policy has been checked against APP. West Midlands Police has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by West Midlands Police.

Those provisions are shown in the links below and can be accessed via the home page of the APP website:

[APP Content](#)

Policy Statements:

- The key components of information & records management are:
 - record collection / creation;
 - record keeping;
 - record maintenance (including tracking of record movements);
 - access and disclosure;
 - closure and transfer;
 - appraisal;
 - archiving; and
 - disposal.
- This policy relates to all information held in any format by the force. These include:
 - All corporate records (e.g. HR, financial, property, accounting, ICT data)
 - All operational and related records
 - All physical records including paper files
 - All electronic records, including data held within IT systems, email records and scanned files

- WMP will comply with the legal and professional obligations set out in national guidance and legislation, in particular:
 - [Management of Police Information \(MoPI\)](#)
 - [The Data Protection Act 2018](#)
 - [The Freedom of Information Act 2000](#)
 - [Criminal Procedure and Investigations Act 1996](#)
 - Any other legislation/requirements which affect records management.
- This policy document must be utilised in conjunction with further advice and guidance found on the [Force Records intranet pages](#).
- WMP will maintain an Information Asset Register. NPU/Departments can register the records they maintain via the Information Asset Owner (IAO).
- The register and associated work streams will be managed and reviewed by Information Management.
- The inventory of record collections will facilitate:
 - The classification of records into series
 - The recording of the responsibility of individuals creating records.

MANAGEMENT OF POLICE INFORMATION (MoPI)

- WMP pay due regard to the Management of Police Information (MoPI) Code of Practice and guidance as published on the College of Policing Authorised Professional Practice (APP) website.
- It is based on current requirements, technical considerations and professional best practice.
- MoPI specifically applies to records associated with the below groups:

Review group	Offence/record type	Action	Rationale
Group 1			
Certain public protection matters	1. MAPPA managed offenders 2. Serious offence specified in CJA 2003 3. Potentially dangerous people	Retain until subject has reached 100 years of age. Review every 10 years to ensure adequacy and necessity.	This category poses the highest possible risk of harm to the public.



Group 2

Other sexual and violent offences	Sexual offences listed in Schedule 3 Sexual Offences Act 2003. Violent offences specified in the Home Office counting rules for recorded crime/ national crime recording standard. This group also includes specified offences that are not serious offences as defined in the Criminal Justice Act 2000. Other serious offences are recorded as such on the PNLD.	Review after an initial 10-year clear period. If subject is deemed to pose a high risk of harm, retain and review after a further 10-year clear period.	National retention assessment criteria
-----------------------------------	---	---	--

Group 3

All other offences	All other offences	Retain for initial 6-year clear period. Either review and risk assess every 5 years or carry out time-based disposal, depending on force policy.	Lower risk of harm. Forces must balance the risk posed by this group with the burden of reviewing.
--------------------	--------------------	---	--

DATA QUALITY

- WMP are committed to managing information successfully.
- We must ensure that all information is recorded properly at the outset to ensure the principles of the Data Protection Act 2018 are followed, which require personal information to be:
 - adequate, relevant and not excessive
 - accurate, relevant and up to date, and
 - kept for no longer than is necessary for its purpose
- The Records Management Team will be involved in Data Quality issues affecting the Force, providing advice, guidance and other data correction functions.

- The Force recognises that data quality is:
 - Integral to effective policing
 - Helps inform better decision making
 - Increases public and officer safety utilising correct, up to date information
 - Can help avoid civil claims and fines
 - Can increase efficiencies around searching / retrieving data
 - Can help avoid missed opportunities, as well as serving legal obligations.

AUDIT AND DIP SAMPLING

- The force will audit / dip sample its information and records management practices for compliance.
- Due to the volume of systems and data assets it is not possible to audit all information, data quality and RM compliance in any given year.
- Instead a risk-based approach is taken. This includes:
 - The data protection risk assessment (from the College of Policing APP)
 - Business continuity feedback
 - Status of the system (e.g. if it is about to be replaced)
 - Home Office initiatives and force priorities.
 - From the results of the risk assessments high risk areas are identified and an audit plan is prepared.
- The audit plan is approved through the Information Assurance Working Group (IAWG) and Strategic Information Management Board (SIMB) governance structure.
- The audit plan is intended to be flexible and expected to change at times in response to events and as agreed between the Assistant Director of Information Management and the Head of Force Records.
- Significant changes are approved by the IAWG or SIMB as appropriate.
- The audits may also be referred to as dip samples or data quality health checks.
- The Information Asset Owner (IAO) will be involved at every stage and responsible for any improvement work, with the support of IM.
- If the resources required to address issues are significant then it may require the involvement of Strategic Tasking, IT&D or the relevant change programmes.
- Additional compliance and monitoring activity is carried out within other business functions that supports records management review. Areas include:
 - Information Security audits
 - Audit & Compliance Team reviews
 - Department supervisor checks
 - Reviews / update and the correction of data
 - Any associated audits carried out by the Internal Audit Team.

- The results of audits will be reported to IAWG and SIMB.

RETENTION AND DISPOSAL SCHEMES

- It is a fundamental requirement that all of the force's records are retained for a minimum period of time for legal, operational, research, practical 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.
- Personal data (and other WMP records) must be reviewed at the end of the specified retention period, and must be destroyed if it is no longer necessary or proportionate to retain the information.
- Records may be held beyond their operationally required retention period for scientific, archiving or historical purposes on a case by case basis (for example, they may be moved to the WMP museum). However, these records will no longer be used to conduct routine WMP business.
- The force has published its WMP retention schedule which can be found on the [Information Management / Force Records intranet pages](#).
- The WMP retention schedule will be reviewed annually and will reflect national retention where appropriate.
- Secure destruction of data must be in accordance with Information Security policies and will be in line with CPNI ([Centre for the Protection of National Infrastructure](#)) national standards.
- The Head of Force Records and the Records Management Supervisor can be contacted for queries and advice.

Definitions/Acronyms:

APP – Authorised Professional Practice
HR – Human Resources
IAWG – Information Assurance Working Group
ICT – Information and Communication Technology
IM – Information Management
IAO – Information Asset Owner
IT & D – Information Technology & Digital
NPU – Neighbourhood Policing Unit
RM – Records Management
SIMB – Strategic Information Management Board
WMP – West Midlands Police

Procedural Guidance Documents List:

Terms & Definitions
Roles & Responsibilities



Publication Instructions:

- **OFFICIAL – Suitable for FOI Publication**

Policy Ref: IM/01

Version: 1.0

Initial Policy Implementation Date: 11/06/2020

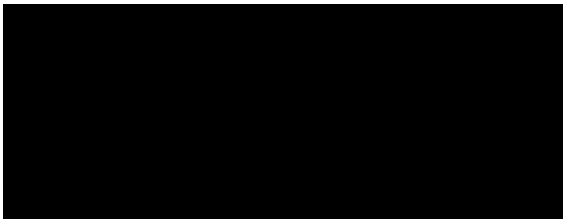
Date: 29/12/2022

Review Date: 29/12/2024

Policy Author: [REDACTED]

Any enquiries in relation to this policy should be made directly with the policy author shown above.

Force Executive Approval:



CHIEF CONSTABLE



Monitoring and Review

Version	Date Reviewed	No change / Minor Changes / Major Changes (<i>detail</i>)	Amended / Agreed by
1.1	29/12/2022	Minor typo corrections, terminology updates, contact update	
1.1	23/03/2023	Policy ref change to reflect department and portfolio change	