



RECORD MANAGEMENT POLICY

Executive Summary

As a public body West Midlands Police (WMP) is required by law to manage our information appropriately and in accordance with legislation and guidance.

Records Management (RM) comprises the processes and controls by which an organisation manages records throughout their lifecycle whether internally or externally generated, including information held within cloud-based, digital and traditional record systems, 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. Effective records management supports transparency, accountability, effective policing and business operations, and compliance with statutory obligations.

WMP 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 Code of Practice. WMP has adopted the Codes provisions, [Police information and records management Code of Practice | College of Policing](#) with supplementary information contained herein, which reflects local practice and the needs of the communities served by WMP.

Scope

The Chief Constable has overall direction and control of WMP and is accountable for all policies and supporting documents of the organisation and its actions. Adherence to this force policy will be expected from all police officers and police staff, all volunteers for the organisation and those working under contract, all employees and representatives of WMP.

Objectives

This policy aims to:

- To ensure there is an appropriate governance structure in place.
- To ensure WMP manages records throughout their lifecycle in a consistent, lawful and efficient manner.
- To support compliance with legislative, regulatory and operational requirement relating to information and records management.
- To ensure records remain authentic, reliable, accessible and usable for as long as required.
- To support effective policing, accountability, transparency and evidence-based decision making.
- To ensure records are retained, reviewed, archived and disposed of in accordance with approved retention schedules and statutory requirements.
- To support the protection of information assets through appropriate governance, security and records management controls.
- To support the effective management of information held in physical, electronic and cloud-based systems.
- To support lawful information sharing.

Definitions/Acronyms

**DEFINITIONS:****Record**

Information created, received and maintained as evidence and information by an organisation or person, pursuance of legal obligations or in the transaction of business (ISO 15489-1:2016)

Although not an exhaustive list, records can include:

Documents and Correspondence

- Contracts, deeds, agreements, judgements and adjudications
- Correspondence, reports and advice given and received
- Memorandum, operating instructions, executive decisions, policies and procedures
- Agendas, minutes, decisions, actions and outcomes of meetings
- Registrations, appointments and announcements
- Personnel records, occupational health records, Development Plans and Professional Development Reviews
- Financial information, invoices, purchase orders, bank statements and monetary transactions
- Intellectual property, patents and trademarks
- Any other necessary documents, communications and information received by the organisation, or generated by the organisation, in the course of conducting its business

Operational and Evidential Records

- Crime, custody and Police National Computer (PNC) records
- Witness statements
- Diary records and pocket notebooks (PNBs)
- Seized evidence (e.g. from mobile phones as well as physical documents)

Electronic Records and Communications

- Computer files (including word processor files, databases, spreadsheets and presentations)
- Electronic mail, text messages and any relevant WMP social media posts.
- Web pages (Intranet and Internet)
- Forms
- Fax
- MS365 content including SharePoint, Teams, OneDrive, OneNote and Power Platform solutions

Audio, Visual and Digital Media

- Digital (interview) recordings,
- Audio and video recordings,
- CCTV recordings
- Body Worn Video (BWV) footage
- Drone/Unmanned Aircraft System (UAS) imagery recordings



	<ul style="list-style-type: none"> • Photographs <p>Specialist and Historic Records</p> <ul style="list-style-type: none"> • Maps and plans • Microfiche and microfilm • Brochures and reports
Personal Information	Information relating to an identified or identifiable living individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier, or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.
Anonymisation	The process of removing personal identifiers so that an individual can no longer by any means reasonably likely to be used.
Pseudonymisation	The processing of personal data so that it can no longer be attributed to a specific individual without the use of additional information held separately.

ACRONYMS:

APP	Authorised Professional Practice
BWV	Body Worn Video
DAB	Data Assurance Board
DPO	Data Protection Officer
FOI	Freedom of Information
HR	Human Resources
IM	Information Management
IA	Information Assets
IAR	Information Asset Register
IAO	Information Asset Owner
IT & D	Information Technology & Digital
LPA	Local Policing Area
RM	Records Management
PNC	Police National Computer
PNB	Pocket Note Book
RRD	Retention Review and Disposal
UAS	Unmanned Aircraft System
SIRO	Senior Information Risk Owner
WMP	West Midlands Police

Policy Statements

1. OVERVIEW

1.1 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.

1.2 This policy applies to all information and records held by WMP, regardless of format, media or location. Further examples of records covered by this policy can be found in the Definitions/Acronyms section

1.3 WMP will comply with the legal and professional obligations set out in national guidance and legislation, in particular:

- [Police Information and Records Management Code of Practice 2023](#)
- [College of Policing Retention, Review and Disposal APP \(this include the Management of Police Information Groups\)](#)
- [UK GDPR](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025 – Amendments to UK GDPR and DPA 2018](#)
- [Freedom of Information Act 2000](#)
- [Criminal Procedure and Investigations Act 1996](#)
- Relevant Home Office, College of Policing and National Archives Guidance
- [Privacy and Electronic Communications Regulations 2003](#) (where applicable)
- Any other applicable legislative or regulatory powers

1.4 This policy document must be utilised in conjunction with further advice and guidance found on the [Force Records intranet pages](#).

2. MANAGEMENT OF POLICE INFORMATION (MOPI)

2.1 WMP pay due regard to the Police Information and Records Management Code of Practice 2023 and associated [Review Retention and Disposal \(RRD\)](#) guidance.

2.2 The Police Information and Records Management Code of Practice 2023 and associated APP guidance are based on current requirements, technical considerations and professional best practice.

2.3 Information subject to Police Information and Records Management Code of Practice 2023 requirements shall be recorded, reviewed and disposed of in accordance with applicable MoPI retention and review criteria

2.4 MoPI specifically applies to records associated with the below groups



Review group	Examples of offences and record type	Action	Rationale
Group 1 – serious offences and public protection matters	<p>Multi-agency public protection arrangements (MAPPA) managed offenders.</p> <p>Offences specified in the Sentencing Act 2020 Schedule 18 which carry a maximum sentence of 10 years or more.</p> <p>Potentially dangerous people.</p>	<p>Having taken into account the retention criteria detailed above, you may retain until the nominal has reached 100 years of age, then carry out a manual review.</p> <p>Review every 10 years to ensure adequacy and necessity.</p>	This category poses the highest possible risk of harm to the public.
Group 2 – other sexual and violent offences	<p>Sexual offences listed in Schedule 3 of the Sexual Offences Act 2003.</p> <p>Violent offences specified in the Home Office counting rules for recorded crime and the National Crime Recording Standard.</p> <p>This group also includes offences specified in Schedule 18 of the Sentencing Act 2020 which are not Group 1 offences, ie, carry a maximum sentence of less than 10 years.</p> <p>Other serious offences are recorded as such on the PNLD.</p>	<p>Review after an initial 10-year clear period.</p> <p>If the subject is deemed to pose a high risk of harm, retain and review after a further 10-year clear period.</p>	NRAC.



Group 3 – all other offences	All other offences.	Retain for an initial six-year clear period, followed by subsequent five-year clear period reviews. Either review and risk assess after a six-year clear period 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.
-------------------------------------	---------------------	--	---

3. INFORMATION ASSET REGISTER (IAR)

- 3.1 WMP maintain an Information Asset Register (IAR) to identify and record information assets and support the effective management of records and information throughout their lifecycle.
- 3.2 The IAR will include relevant information about information assets, including ownership, the systems of locations in which records are held, the nature of the records and information processed, and relevant retention, review disposal and protection arrangements.
- 3.3 Information Asset records must be reviewed annually and as required following any significant changes to systems, processing activities, legislation or business requirements.
- 3.4 Information Assets will be assigned an IAO. Information Asset Owners (IAO) are responsible for overseeing that information assets, within their area of responsibility, are recorded within the IAR, retention requirements are applied, records are reviewed in accordance with approved schedules, appropriate disposal methods are undertaken, and for identifying and managing acceptable information risks.
- 3.5 Access to the IAR is restricted to authorised personnel only although it may be suitable for publication through The Freedom of Information Act 2000 (FOI) once redacted.

4 ACCESS TO RECORDS

- 4.1 Access to force records, information and systems shall be restricted to authorised personnel with a legitimate operational, business or legal requirement. Access permissions is role-based, proportionate to the user's responsibilities.
- 4.2 IAOs are responsible for defining appropriate business access requirements for information assets within their area of responsibility.
- 4.3 Access to systems should be reviewed regularly and amended or removed promptly when personnel change roles, leave the Force or no longer require access.



- 4.4 Access to physical records held on Force premises or within approved off-site storage facilities shall be restricted to authorised personnel. Requests for physical records shall be logged and managed through the Records Management team.
- 4.5 Access to records may be provided to internal or external parties where there is a lawful, necessary and proportionate reason to do so in accordance with applicable legislation, Force (and or national??) policies and approved information sharing agreements.
- 4.6 Any record requests should be requested by using the [File Request Form](#) or email at: [REDACTED]

5 DATA QUALITY

- 5.1 WMP is committed to maintaining accurate, complete, relevant and reliable records to support effective policing, decision making and compliance with legal and regulatory requirements.
- 5.2 Records must be created, maintained and reviewed in a way that ensures information is accurate, relevant, complete and, where necessary, kept up to date. Where records containing personal information, they must also be managed in accordance with applicable data protection legislation.
- 5.3 The Records Management Team will provide advice, guidance and support on data quality issues affecting the Force.
- 5.4 The Force recognises that data quality:
- Is integral to effective policing
 - Supports effective decision making, safeguarding, investigations, public confidence and legal compliance
 - Increases public and officer safety utilising correct, up to date information
 - Can help reduce the risk of operational errors, legal challenges, regulatory action and reputational damage.
 - Can increase efficiencies around searching / retrieving data
 - Can help avoid missed opportunities, as well as serving legal obligations.
- 5.6 Any officers, staff members, volunteers, contractors or other authorised users who identifies an error, inaccuracy, omission or other data quality issues with a Force record or system must take appropriate action to ensure it is reported and addressed. This may include correcting the information where authorised, raising the information through the relevant support process, escalating to a manager or supervisor, or seeking advice from Information Management or Records Management Team.
- 5.7 WMP will take reasonable steps to ensure that inaccurate, incomplete or out of date records are identified and corrected without undue delay. Requests to rectify personal information will be managed in accordance with data protection legislation and relevant National procedures. Where a record cannot be amended, the reason for this and any relevant challenge, correction or supplementary information should be recorded appropriately.
- 5.8 For all rectification requests, email [REDACTED]
- 5.9 External use only: [West Midlands Police - Ask for delete or change information](#)



6 MONITORING, ASSURANCE AND AUDIT

- 6.1 WMP will undertake proportionate monitoring, assurance and review activities to assess compliance with records management requirements.
- 6.2 Monitoring assurance and review activities will be proportionate and risk-based, taking into account operational, organisational, legislative and information management risks.
- 6.3 Information Asset Owners and relevant business areas will support monitoring and assurance activities and address identified improvement actions.
- 6.4 Findings, recommendations and improvement action plans arising from monitoring and assurance activities will be reported through the appropriate governance arrangements.

7 REVIEW RETENTION AND DISPOSAL (RRD)

- 7.1 It is a fundamental requirement that all of the force's records are retained for as long as necessary for the purpose for which it was collected.
- 7.2 The length of time for retaining records will depend on the type of record and its importance to the force's business functions. A review at the end of that specified retention period will occur resulting in either the destruction or retention of the record.
- 7.3 The review, retention and destruction of physical records shall be undertaken in accordance with the Force Retention Schedule and the [Review Retention and Destruction of Retained Documents Policy](#).
- 7.4 Where technically feasible, automated or system supported review, retention and disposal controls may be used to support compliance with approved retention schedules, subject to appropriate governance, assurance and audit arrangements
- 7.5 Records may be retained beyond their operational retention period where we can demonstrate an on-going need for continued access to the data for policing purposes. This non-standards retention will be documented on an [NRAC form](#). The Records Management team will complete these forms and maintain a log for audit trail purposes.
- 7.6 Records may also be retained for archiving in the public interest, scientific research, historical research or statistical purposes on a case-by-case basis, where appropriate and in accordance with legislative requirements.
- 7.7 Where necessary and proportionate, measures such as anonymisation and pseudonymisation maybe applied. However, these records will not normally be used to conduct routine WMP business.
- 7.8 WMP follow the [NPPC national retention schedule](#). Whenever the national retention schedule is re-issued, WMP will review it and if necessary, supplement with additions.



8 TRAINING

- 8.1 WMP will ensure that officers, staff, volunteers, contractors and other authorised users receive appropriate records management awareness, training and guidance relevant to their role. This will include record management awareness through the CoP induction process mandatory training for all new and existing personnel and additional learning to support compliance with records management obligations.
- 8.2 IAO will be provided with specific training to ensure they are aware of their role and responsibilities.

9 ROLES AND RESPONSIBILITIES

9.1 Chief Constable

- The Chief Constable has overall accountability for ensuring WMP manages and records information in accordance with legislative, regulatory and operational requirements

9.2 Senior Information Risk Owner (SIRO)

- The Senior Information Risk Owner (SIRO) provides strategic oversight of information and records management and ensures that information risks are identified, managed and escalated quickly. The SIRO may appoint a deputy who must be someone of suitable seniority with the same authorisation to make decisions on their behalf.

9.3 Information Asset Owners (IAOs)

- IAOs have overall accountability for the information assets within their area of responsibility. They are responsible for ensuring that information assets are appropriately governed, protected and managed throughout their lifecycle, including the application of appropriate retention, review and disposal arrangements.

9.4 Information Assets

- Information Assets shall be recorded within the Information Asset Register and assigned to an IAO. Information Asset Register entries should remain accurate, complete and up to date. Regular reviews should be conducted and entries reviewed following significant changes to ownership, processing activities, retention requirements or identified risks.

9.5 Information Management Lead

- The Information Management Lead is responsible for the development, implementation and monitoring of records management policies, standards and procedures. Provides advice and guidance to the Force, supports assurance and compliance activities, maintains the Information Asset Register and sets strategic objectives for the organisation to improve record management best practices.

9.6 Data Protection Officer (DPO)

- The Data Protection Officer provides independent advice and guidance on data protection legislation and support compliance with statutory obligations relating to personal data. They act as a point of contact for regulatory authorities and manage data protection impact assessments.

9.7 Records Manager / Record Management Team

- The Records Manager and Records Management Team provide professional advice, guidance and support on records management matters. This includes maintaining



records management standards, supporting retention and disposal activities, promoting good practice and assisting with records management assurance activities working alongside business areas.

9.8 Managers – All Business Areas

- Managers are responsible for ensuring staff within their area understand and comply with records management requirements and receive appropriate support and guidance where necessary.

9.9 All Users

- All officers, staff, volunteers, contractors and other authorised users who create, receive, access or manage records are responsible for ensuring records are accurate, complete, secure and managed in accordance with this policy and associated guidance.
- All users are responsible for maintaining data quality, avoiding unnecessary duplication of records and ensuring information is recorded in a timely manner.

Relevant Legislation / Policies / Procedural Guidance

- [NPPC national retention schedule.](#)
- [Review Retention and Destruction of Retained Documents Policy.](#)
- [Review, retention and disposal | College of Policing](#)
- [Police Information and Records Management Code of Practice 2023](#)
- [College of Policing Retention, Review and Disposal APP \(this include the Management of Police Information Groups\)](#)
- [UK GDPR](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025 – Amendments to UK GDPR and DPA 2018](#)
- [Freedom of Information Act 2000](#)
- [Criminal Procedure and Investigations Act 1996](#)
- [Privacy and Electronic Communications Regulations 2003](#)

Equality Impact Assessment

WMP places trust in their employees to comply with force policies and to work in accordance with and in support of:

- [WMP Vision and Values](#)
- [Code of Ethics | College of Policing](#)
- [Voice of the Child](#)

	What impact has this policy had on the nine protected characteristics in relation to the three general duties? (If applicable)	How will this updated policy positively impact each of the nine protected characteristics in relation to the three general duties? If not, explain why it will not.
Age (including children and young persons)	No impact	N/A – no anticipated positive impact



Disability	No impact	No anticipated positive impact. The Reasonable Adjustments process covers any adjustments that need to be made.
Gender Reassignment	No impact	N/A – no anticipated positive impact
Pregnancy & Maternity	No impact	N/A – no anticipated positive impact
Marriage & Civil Partnership	No impact	N/A – no anticipated positive impact
Race	No impact	N/A – no anticipated positive impact
Religion or Belief	No impact	N/A – no anticipated positive impact
Sex	No impact	N/A – no anticipated positive impact
Sexual Orientation	No impact	N/A – no anticipated positive impact

Publication Instructions

Suitable for publication to public

Document Control

Strategic Lead: <i>[role and name]</i>	
Policy Author(s): <i>[role and name]</i>	
Effective Date:	30/06/2026
FET Lead: <i>[role and name]</i>	Peter Gillett - Director of Commercial Services
Version Number:	2.0
Review Date:	30/06/2030

Any enquiries in relation to this policy should be made directly with the Strategic Lead.

All policies are subject to a formal consultation process which encompasses Legal, Professional Standards, Faith Groups, Trade Unions, Independent Advisory Groups and wider force groups and any other relevant parties. A record of consultation can be found on the Policy Portal.

It is responsibility of the Strategic Lead to ensure that all links within the policy are correct and accessible.

Amendment History:

Version Number:	Effective Date:	Summary of Amendments:	Author:
2.0	29/06/26	Revised version due to policy expiry	

Official

