

OPERATIONAL AND CORPORATE NOTES

Executive Summary:

As a public body WMP are required by law to manage information and records appropriately and in accordance with legislation and guidance. This obligation extends to all notes taken by WMP staff, including- but not limited to- all operational notes relating to investigations, cases and operations, all corporate notes relating to the functioning of WMP, and all notes made by staff and officers in the course of their daily activities.

The Force's notes provide intelligence, evidence, a history of actions, decisions and represent a vital asset to support daily functions and operations. Failure to comply with correct handling can compromise WMP activities and can lead to serious consequences. By placing such controls around notes, we can ensure our information demonstrates the key attributes of authenticity, reliability, integrity and accessibility. This policy also supports consistency, continuity, efficiency and productivity.

Authorised Professional Practice (APP):

(*delete as appropriate)

- This policy has been checked against APP and West Midlands Police has adopted the provisions of APP as its policy.

Those provisions are shown in the link(s) below and can be accessed via the home page of the APP website:

<https://www.app.college.police.uk/app-content/information-management/>

Policy Statements:

NOTES FORMATS

- This policy relates to all notes held in any format by the force:
 - All corporate notes (e.g. HR, financial, property, accounting)
 - All operational and related notes
 - All physical notes including paper printouts, notebooks and loose notes
 - All electronic notes, including data held within IT systems, emailed notes and scanned notes.

MANAGING INFORMATION HELD IN NOTES

- The key components of the correct handling of notes are:
 - **Capture & Transfer:** Notes are identified correctly and held in the correct format.
 - **Disclosure, Access & Oversight:** Notes are disclosed upon request during investigations and under relevant legislation. Notes are shared appropriately when necessary.
 - **Security:** All notes are held securely in compliance with relevant physical and electronic security standards. This includes secure storage, damage and loss prevention, secure management of movement and transport.

- **Retention, Review and Destruction:** Notes are retained according to the relevant retention period, reviewed for accuracy and relevance, and destroyed correctly at the end of life (or transferred for historical retention).

LEGISLATION AND GUIDANCE

- WMP will comply with the legal and professional obligations set out in national guidance and legislation, in particular:
 - [Management of Police Information \(MoPI\)](#)
 - [The Government Security Classifications](#)
 - [The Data Protection Act 2018](#)
 - [The Freedom of Information Act 2000](#)
 - [Criminal Procedure and Investigations Act 1996](#)
 - [The Inquiries Act 2005](#)
- Any other legislation/requirements which affect records management and the secure handling of information.
- This policy document should be utilised in conjunction with:
 - Handling Notes Procedural Guidance
 - [Force Records Management advice and guidance](#)
 - [Records Management Policy](#)
 - [Information Security Policy & documents](#)
 - [Information Risk Management Policy](#)
 - Policy & guidance on the integrity of evidence and investigations
 - The WMP Retention schedule

Definitions/Acronyms:

Management of Police Information (MoPI)

The principles of Management of Police Information (MoPI) provide a way of balancing proportionality and necessity and are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information:

- Collection & recording
- Evaluation
- Common process
- Review, retention & disposal

Police information is information recorded for a policing purpose.

Policing purpose applies to:

- 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.

Records are defined as recorded information and documentation, in any form, created or received and maintained as evidence and information by the force or an individual, in the pursuance of legal obligations or transaction of its business or conduct of affairs and kept as evidence of such activity.

Records can be in any format, irrespective of the technology used to create and store them or the type of information they contain. It is the managed and structured environment within which records should be held which gives the information they contain context and authenticity as reliable and complete evidence of past actions and decisions.

The Force's records are important sources of administrative, evidential and historical information. They are vital to the force to support its current / future operations and to meet legal obligations including the Data Protection Act 2018, Criminal Procedure & Investigation Act 1996 & Freedom of Information legislation. They are also vital to ensure compliance with MoPI and for the purpose of accountability, and for an awareness and understanding of its history and procedures.

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage, disposal, destruction or preservation 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.

Information Security exists to protect WMP information assets from all threats, whether internal or external, deliberate or accidental. It is concerned with the preservation of:

- Confidentiality - ensuring that information is accessible only to those authorised to have access, disclosed only to those authorised to receive it, and so disclosed only for police purposes;
- Integrity - safeguarding the accuracy and completeness of information and information processing methods, and the ability to identify anomalies;
- Availability - ensuring that authorised users have access to information and associated assets when required.

Retention is the controlled possession, use and storage of information.

Review means to assess a record to determine whether it still has a policing, legal or other business purpose to be retained, ensure that it is adequate, relevant, accurate and up to date for the purpose for which it is held.

Disposal / Destruction means to delete or securely destroy a record when its disposal period has been reached and it no longer has a policing, legal or other business purpose.

Procedural Guidance Documents List:

- Attached Procedural Guidance
- [Force Records Management advice and guidance](#)
- [Records Management Policy](#)
- [Information Security Policy & documents](#)
- [Information Risk Management Policy](#)
- Policy & guidance on the integrity of evidence and investigations

Publication Instructions:

- Suitable for publication to public

Policy Ref: COM/08

Version: 1.0

Date: 04/03/2021

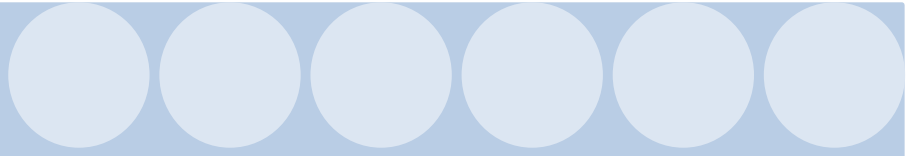
Review Date: 04/03/2022

Policy Author: Karen Gaille

Any enquiries in relation to this policy should be made directly with the policy contact 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	New review date