



# LAWFUL BUSINESS MONITORING POLICY

## Executive Summary

The [Investigatory Powers \(Interception by Businesses etc. for Monitoring and Record-keeping Purposes\) Regulations 2018](#) allows West Midlands Police (WMP) to monitor and intercept transactions made on work systems and/or devices. This legislative framework allows WMP to review the activity of users on non-private systems/devices to check that it is legal and follows an expected level of conduct. This is a practice also known as and referred to as Lawful Business Monitoring (LBM)

This policy is a key component of WMP's overall approach to protecting information and should be considered alongside more detailed information security documentation including relevant security guidance and procedures (including the [Information Security Policy](#)).

## Authorised Professional Practice (APP)

This policy has been checked against APP and there is none in relation to the subject matter of this policy.

## 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 employees and representatives of WMP

## Objectives

This policy aims to:

- Outline WMP's actions in identifying potential criminality or misconduct using policing systems/devices/machines/software
- Outline expectations around the use of WMP communication systems, which are for official WMP business only.
- Inform WMP staff and officers, contractors or other users of WMP provided systems/devices/machines/software that all activity can be recorded and monitored legally.
- Ensure all staff and officers are aware of the legislation that allows this monitoring and recording to take place.
- Remind all staff that the capability to monitor and record staff is to allow the ongoing protection of the public.
- Reassure staff that, despite the legislative framework to allow monitoring and recording, all investigative work conducted by Professional Standards Department (PSD) staff will be scrutinised by appropriate consent levels being in place, with the ethics and proportionality of any intrusion being considered.
- Formalise the structure of requests by PSD to monitor/record/review any information.
- Outline the use of lawful business monitoring from an investigative perspective. Any data quality or other audits are considered within the [Information Security Policy](#).

## Definitions/Acronyms



|            |                                   |
|------------|-----------------------------------|
| <b>APP</b> | Authorised Professional Practice  |
| <b>CPS</b> | Crown Prosecution Service         |
| <b>LBM</b> | Lawful Business Monitoring        |
| <b>PSD</b> | Professional Standards Department |
| <b>WMP</b> | West Midlands Police              |

## Policy Statements

### 1. OVERVIEW

- 1.1 The use of the LBM policy will reduce risk and improve performance in the following areas:
- Investigations of internal systems misuse
  - Staff training and development
  - Business continuity
  - Evidence gathering in criminal investigations
  - Integrity of Police communication systems
- 1.2 Under LBM, WMP can monitor (store and retrieve) and intercept (observe live) all transactions made on services and equipment provided to enable, facilitate, and/or conduct business on behalf of WMP.
- 1.3 Monitoring and recording include, but is not limited to, use of any systems, devices, machines and software that are owned/provided by/accessed via:
- WMP internet provision and any website accessed (including social media, banking, non-police email)
  - WMP mobile phones/tablets/devices
  - WMP computer systems
  - WMP vehicles
  - WMP police radios
  - This includes all information transmitted to and from the above, including geolocation data.
- 1.4 WMP staff and officers have responsibilities when using WMP systems/devices and all activity can be monitored and used for criminal or misconduct investigations.
- 1.5 Usage of police communication systems, including for personal use (please see below) must conform to the [Code of Ethics](#).
- 1.6 A number of conditions need to be met to allow the use of Lawful Business Monitoring:
- The system controller must make all reasonable efforts to inform potential users that interceptions may be made **and**;
  - The activity needs to have one of the following purposes:
    - Establishing facts
    - Ascertain compliance with practices or procedures
    - Maintain and measure standards
    - In the interests of national security



- To prevent/detect crime
- Detecting any unauthorised use of the system
- To secure, or as an inherent part of, effective system operation

1.7 At WMP, all staff and officers are aware of the way in which they are expected to use the systems that they are given access to. This is reinforced by:

- This policy
- The Acceptable Use Statement upon login of desktops
- The login screen on laptops
- User forms for WMP mobile devices, signed by users
- Acceptable use reiterated on various other systems
- Terms of employment

1.8 There is an understanding that staff may make occasional and reasonable personal use of the provided communications systems (email, telephone, internet etc.).

1.9 Reasonable use does not include behaviours such as, but not limited to, discriminatory language or hate speech, foul language, protracted non-work conversations and any communications relating to intimate personal relationships.

1.10 Communications including personal use across these systems can be observed and/or recorded.

1.11 For private non-work-related matters, personal communication devices should be used.

1.12 It is accepted that, as with any investigative technique, there may be 'collateral intrusion' through LBM

1.13 This includes the discovery of sensitive data, personal information and other material not sought as part of the original rationale for the tactic.

1.14 In these circumstances the principle set out in '[The Employment Practices Code](#)' shall be followed: "disregard and where feasible delete other information collected in the course of monitoring unless it reveals information that no employer could reasonably be expected to ignore."

1.15 However, if the material is gathered in response to a criminal investigation, then it will be retained securely.

1.16 This is in line with the disclosure guidelines published by the Crown Prosecution Service (CPS) and embodied within the [Criminal Procedure and Investigations Act 1996](#) as amended by the [Criminal Justice Act 2003](#) and the revised Code of Practice issued under it

## 2. GOVERNANCE

2.1 [Investigatory Powers \(Interception by Businesses etc. for Monitoring and Record-keeping Purposes\) Regulations 2018](#) refers to a "system controller".

2.2 In relation to a particular telecommunication system, a system controller is a person with a right to control its operation or use.



2.3 WMP interprets that this can be the Chief Constable or Deputy Chief Constable in view of their ownership, oversight and understanding of the systems utilised by WMP.

2.4 The Deputy Chief Constable has authorised the use of LBM in WMP.

### 3. HUMAN RIGHTS

3.1 The use of Lawful Business Monitoring must be compatible with all of the human rights articles as set out in the [European Convention on Human Rights](#).

3.2 This policy has the potential to engage the following qualified articles:

- Article 8 – Right to respect of private or family life
- Article 9 – Freedom to manifest your religion or belief
- Article 10 – Freedom of expression

3.3 Qualified rights may be restricted within the following circumstances:

- National security
- Public safety
- Economic well-being of the country.
- For the prevention of disorder or crime.
- For the protection of health and morals.
- For the protection of the rights and freedoms of others.

3.4 The restriction made must be proportionate to the need.

3.5 Subject to proportionality, restriction of these qualified rights may be necessary for WMP to:

- Be effective
- Protect the public
- Maintain high standards of conduct and integrity from its staff and officers
- Protect the legitimacy and reputation of WMP.

## Relevant Legislation / Policies / Procedural Guidance

- [Government Security Classification Procedure](#).
- [Data Protection](#)
- [Information Management Policy](#)
- [Standards of Professional Behaviour](#)
- [Investigatory Powers \(Interception by Businesses etc. for Monitoring and Record-keeping Purposes\) Regulations 2018](#)
- [Information Security Policy](#)
- [Code of Ethics](#).
- [Criminal Procedure and Investigations Act 1996](#)
- [The employment practices code](#)
- [Criminal Justice Act 2003](#)
- [European Right on Human Convention](#)



## 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 <b>had</b> on the nine protected characteristics in relation to the three general duties? (If applicable) | How <b>will</b> 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. |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Age<br/>(including children and young persons)</b> | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate.           |
| <b>Disability</b>                                     | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate.           |
| <b>Gender Reassignment</b>                            | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate.           |
| <b>Pregnancy &amp; Maternity</b>                      | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate.           |
| <b>Marriage &amp; Civil Partnership</b>               | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate.           |
| <b>Race</b>                                           | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate.           |
| <b>Religion or Belief</b>                             | There is no known specific impact brought about as a result of this policy.                                                           | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to                                                                         |



|                           |                                                                             |                                                                                                                                                                  |
|---------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           |                                                                             | feel confident in their behaviours with WMP's digital estate.                                                                                                    |
| <b>Sex</b>                | There is no known specific impact brought about as a result of this policy. | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate. |
| <b>Sexual Orientation</b> | There is no known specific impact brought about as a result of this policy. | The policy outlines expectations already highlighted to WMP staff and volunteers, allowing them to feel confident in their behaviours with WMP's digital estate. |

## Publication Instructions

Suitable for publication to public

## Document Control

|                                                    |                                                                                                       |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Strategic Lead:</b><br><i>[role and name]</i>   | ██████████ – D/Supt - PSD                                                                             |
| <b>Policy Author(s):</b><br><i>[role and name]</i> | ██████████ – CI - Senior Investigation Manager<br>██████████ - Counter Corruption Unit - Intelligence |
| <b>Effective Date:</b>                             | 17/06/26                                                                                              |
| <b>FET Lead:</b><br><i>[role and name]</i>         | T/DCC Mattinson                                                                                       |
| <b>Version Number:</b>                             | v3.0                                                                                                  |
| <b>Review Date:</b>                                | 17/06/2030                                                                                            |

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:                  |
|-----------------|-----------------|---------------------------------------------------------------|--------------------------|
| 3.0             | 30.04.2026      | Scheduled review – minor amends of terminology and formatting | ██████████<br>██████████ |