LAWFUL BUSINESS MONITORING

Executive Summary:

This policy is intended to outline expectations around the use of West Midlands Police (WMP) communication systems, which are for official WMP business only.

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).

The aim of this policy is to outline WMP's actions in identifying potential criminality or misconduct using policing systems/devices/machines/software:

- Informing WMP staff and officers, contractors or other users of WMP provided systems/devices/machines/software that all activity can be recorded and monitored legally.
- Ensuring all staff and officers are aware of the legislation that allows this monitoring and recording to take place.
- Reminding all staff that the capability to monitor and record staff is to allow the ongoing protection of the public.
- Reassuring staff that, despite the legislative framework to allow monitoring and recording, all investigative work conducted by PSD staff will be scrutinised by appropriate consent levels being in place, with the ethics and proportionality of any intrusion being considered.
- Formalising the structure of requests by PSD to monitor/record/review any information.
- Outlining the use of lawful business monitoring from an investigative perspective. Any data quality or other audits are considered within the Information Security Policy.

Policy Statements:

- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 allows 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.

- Under Lawful Business Monitoring, 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.

- Monitoring and recording includes, 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.

- WMP staff and officers have responsibilities when using WMP systems/devices and all activity can be monitored and used for criminal or misconduct investigations.

- Usage of police communication systems, including for personal use must conform to the Code of Ethics.

- 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

- 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

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

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

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

- It is accepted that, as with any investigative technique, there may be collateral intrusion through Lawful Business Monitoring.

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

- 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."

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

- This is in line with the disclosure guidelines published by the 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

GOVERNANCE

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

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

- WMP interprets that this can be the Chief Constable or, as the Senior Information Risk Owner, the Deputy Chief Constable.

- The Deputy Chief Constable has authorised the use of Lawful Business Monitoring in WMP.

BENEFITS OF LAWFUL BUSINESS MONITORING

- The use of the Lawful Business Monitoring 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

HUMAN RIGHTS

- 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.

- 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

- 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.

- The restriction made must be proportionate to the need.

- 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.

Definitions/Acronyms:

WMP – West Midlands Police
PSD – Professional Standards Department
CPS – Crown Prosecution Service

Associated Documents:

- *Acceptable Use Procedure*
- *Government Security Classification Procedure.*
- *Data Protection Policy*
- *Information Security Policy*
- *Information Management Policy*
- *Standards of Professional Behaviour*
- *The Employment Practices Code*

Publication Instructions:

e.g. OFFICIAL – Suitable for FOI Publication

Policy Ref: DCC/01

Version: 1.0

Date: 06/09/2021

Review Date: 06/09/2022

Policy Author: Peter Baghurst

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

Force Executive Approval:

CHIEF CONSTABLE

Monitoring and Review

Version	Date Reviewed	No change / Minor Changes / Major Changes *(detail)*	Amended / Agreed by	New review date