Access and Monitoring Force Systems

Contents

Policy Statement 2
Responsibilities 2
All Individuals 2
Line Managers 3
Professional Standards Directorate (PSD) 4
Auditing and Monitoring 4
Lawful Business Monitoring 5
Live Monitoring 5
Personal/Business Use/Expectation of Privacy 5
Force Undertaking on Accessing and Disclosure of Data 6
Maintaining Battery Charge on Force Devices 6
Additional Information 8

Policy Statement

Summary

All users of West Yorkshire Police (WYP) IT systems and devices have a responsibility to access and use them both legally and in line with force policy.
Therefore, the aims of this policy are to ensure all employees are aware of their responsibilities and the expectations placed upon them to safeguard the confidentiality, integrity and availability of information. To explain the framework for the ethical monitoring, interception and recording of communications within the workplace which are transmitted using West Yorkshire Police systems, including Lawful Business Monitoring (LBM).

Scope

This policy applies to all individuals who use Force communication and data storage systems including police officers, police staff, police community support officers (PCSOs), special constables, volunteers, temporary staff, agency staff, ex-employees and any contractors.

Responsibilities

All Individuals

Responsibilities

- The provisions of this policy apply to force issues mobile devices, desktops, laptops, tablets and associated devices with the ability to access force systems that individuals may use as part of their role.
- All individuals must adhere to the following policies when using WYP force systems and devices:
  - Mobile Data Devices, specifically the 'Conditions of Use form' detailed within, that all individuals must agree to and sign prior to the issue of any device;
  - Force web and social media sites
  - Information and Data Management – Data Protection and Information Sharing
  - Information and Data Management – Data Quality, Collection, Storage and Disposal
  - Information and Data Management – Information Security
  - IT security;
  - Using the internet and social media; and
  - Information and Technology Usage.
- Prior to accessing any WYP systems all users must be familiar with the data protection, information security and information and technology usage policies. They must also complete the e-learning package "Use of Police information and Systems".

- All users must abide at all times to the Standards of Professional behaviour as defined by the Police Conduct Regulations 2012 for Officers and the Police Staff Code of Conduct for Staff.
- All users must report any concerns regarding the misuse of force systems or devices to their line manager or Professional Standards Directorate (PSD). This can be done either directly or through the provisions of the confidential reporting mechanisms e.g. anonymous messenger.
- All users must complete the Data Protection Mandatory e-learning training.

Line Managers

Responsibilities – Access to Personal Emails and Data Storage Areas

- There will be occasions when a mailbox or data storage area such as OneDrive or computer desktops will need to be accessed by line managers, such as when absence is short notice and unplanned. It is advised that individuals allow their line manager access, as the authority can be withdrawn at any time.
- Line managers are responsible for:
  - Submitting a request via the IT Self Service Portal for permission of access;
  - Applying an 'Out of Office' reply with appropriate wording;
  - Appointing a designated person access to the mailbox to deal with existing messages;
  - Ensuring relevant emails can be identified and forwarded to the appropriate recipient by the IT Department;
  - Reviewing access in respect of necessity, proportionality and collateral intrusion;
  - Notifying IT Self Service Portal without any undue delay, when access is no longer required; and
  - Informing the owner that access has been granted to their mailbox or data storage area when they return to work;
- The designated person must always consider any issues of confidentiality and legal privilege that may be contained within email messages and deal with them accordingly.
- Any access to mailboxes or data storage areas is granted for 14 days, then a new request must be submitted for further access time.
- When granted access, items from the mailbox or data storage area can be forwarded or saved elsewhere, as required, however items must not be deleted.
- If the owner of the mailbox or data storage area is a representative of either the: Police Federation; Trade Union; or Superintendents Association, then the Federation or Superintendents Association Chair or Secretary, or the Union Branch Secretary must be consulted before the mailbox or data storage area is accessed.

Responsibilities – Suspects Misuse

- In cases where the line manager is accessing for suspected misuse then they are responsible for:
  - Submitting a report to the Head of PSD, requesting access to the mailbox or data storage area due to suspected misuse. Individuals must consider:
  - Necessity;
  - Proportionality;
  - How collateral intrusion is to be minimised; and
  - Circumstances leading to the request.

Professional Standards Directorate (PSD)

Responsibilities

PSD, including the Counter Corruption Unit are responsible for:

- Completing the application of Lawful Business Monitoring, accessing audit information for the purpose of criminal or disciplinary investigations including any allegations of the misuse of force systems.

Auditing and Monitoring

Principles

- The force records and retains information in line with the records management policy and schedule.
- The force records and retains **ALL** transactions undertaken by its employees on **ALL** force systems in order to:
  - Review standards of training or service delivery;
  - Review standard operating procedures or Force policy, procedures or guidance;
  - Ascertain compliance and demonstrate that the required standards are maintained; or
  - Consider or instigate criminal or disciplinary proceedings.
- Monitoring includes electronic communications, e.g. telephone calls, SMS, emails and internet access on systems such as (but not limited to) Outlook accounts, storage drives, work mobile phones, electronic pocket notebooks, computer terminals work laptops, and tablets.
- The data retained will include time and date, details of any recipient such as telephone number or e-mail address and in the case of SMS message content. Should the force seek to provide access to social media applications or other messaging services the content of these will also be retained.
- Data retention will comply with the force records management policy, relevant guidance and the Data Protection Impact assessment.
- The audit and monitoring of employee's activity is outlined within:
  - The Data Protection Employment practice guide;
  - The Information Compliance Office employment practice code;

- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 - conferred by section 46(2) of the Investigatory Powers Act 2016(1); and
- Relevant force policies as outlined above.

Lawful Business Monitoring

Principles

- Lawful business monitoring is outlined within the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018. It includes:
  - The obtaining of "historic" data and information to enable an audit of an individual's activity within the Force's communications systems; and
  - Interception, i.e. the "live" recording of, or the listening to conversations or communications and can involve the recording of anything witnessed.
- Both can extend to off duty use of Force communications systems.
- There can be no monitoring or recording of personal or public telephone networks under lawful business monitoring.
- Whilst the activity is authorised within Lawful Business Practice regulations additional processes are in place to provide reassurance, audit and transparency.
- A NPCC representative or a delegated person will only authorise access when necessary, proportionate and will ensure a record of this authority is maintained.

Live Monitoring

Principles

- The force has the capability to 'live monitor' staff's activity on force systems. However, this would be assessed as 'surveillance' and would only be conducted when there is a criminal investigation and the necessary, authorities are in place and agreed through the force authorising officer in line with RIPA (2000) or the Investigatory Powers Act 2016.
- Live monitoring would not be considered for misconduct investigations only.

Personal/Business Use/Expectation of Privacy

Principles

- All West Yorkshire Police IT devices are issued, and all IT systems are used on the condition that they are used for a Policing Purpose and in the course of your duties or otherwise approved by force policy.
- As communications will be recorded and may be monitored, officers and staff should be aware that their right to privacy is limited and intrusion can

take place where justified and proportionate, when using West Yorkshire Police devices and systems.

- Emergency personal use is permitted when it is related to a Policing Purpose, this would include occasions when you need to contact a family member to inform them that you have been retained on duty or a change in work related matters
- Should you choose to use any IT system outside of these conditions (i.e. for personal use and non-policing purpose) then this policy would be breached. Furthermore, to comply with the Data Protection Act 2018 and General Data Protection Regulations 2018, you are responsible for advising third parties the communications will be recorded and may be monitored and used by West Yorkshire Police for lawful purposes.
- The ONLY exemption to this policy and the use of IT devices for personal use is with written authority from the Senior Information Responsible Officer (SIRO).

Force Undertaking on Accessing and Disclosure of Data

- All staff must be reassured that the access and disclosure of monitoring information will be strictly restricted, it will only be accessed and disclosed when necessary and the level of intrusion will be proportionate to the issue being considered.
- The following protections will be put in place:
  - A privacy impact assessment will be in place and comply with ICO and data protection guidelines;
  - Only a small number of staff within PSD and the Counter Corruption Unit will have access to the audit system;
  - PSD will only access data as part of intelligence development supporting either a disciplinary or a criminal investigation. There will be no speculative or random searching on employees and all access must be justified and approved through a line manager;
  - Levels of authority will be put in place based on the privacy impact assessment and level of intrusion;
  - Access to the system will be audited and made available for any Office of the Surveillance Commissioner (OSC) inspection; and
  - Information assessed under these provisions may be disclosed and relied upon in related criminal or disciplinary proceedings.

Maintaining Battery Charge on Force Devices

Principles

- You will be issued with your own standard charging unit and it is your responsibility to ensure that your device's charge is maintained.

- There is no mandatory requirement to take the device home, but you are allowed to take it home. However, it is anticipated that this will be regular practice to maintain the battery charge. Whenever the device is not in use, you should switch it off and store it as instructed.

Additional Information

Compliance

This policy complies with the following legislation, policy and guidance:

- Data Protection Act 2018
- GDPR 2018
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Police Conduct Regulations 2012
- Police Staff Code of Conduct for Staff
- Mobile Data Devices policy
- Force web and social media sites policy
- Information and Data Management – Data Protection and Information Sharing
- Information and Data Management – Data Quality, Collection, Storage and Disposal
- Information and Data Management – Information Security
- IT security
- Using the internet and social media
- Information and Technology Usage
- The Data Protection Employment practice guide
- The Information Compliance Office employment practice code
- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 - conferred by section 46(2) of the Investigatory Powers Act 2016(1).