

Acceptable Use Policy		
Security Classification	OFFICIAL	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	Acceptable Use Policy
REFERENCE NUMBER	WMP107
Version	2.0

POLICY OWNERSHIP	
DIRECTORATE	BUSINESS SERVICES
BUSINESS AREA	DIGITAL SERVICES

INITIAL IMPLEMENTATION DATE	November 2020
LATEST REVIEW DATE	November 2022
NEXT REVIEW DATE:	November 2025
RISK RATING	LOW
EQUALITY ANALYSIS	LOW

West Mercia Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy.
Please e-mail policiesandprocedures@westmercia.police.uk

Handling Instructions

OFFICIAL - This document must be handled and stored according to the Government Security Classifications guidance. Neither the document nor any of its contents may be disseminated further without the permission of the Information Asset Owner.

1.0 POLICY OUTLINE

The Acceptable Use Policy is used to establish rules for the acceptable use of West Mercia Police's (WMP) information and assets by all those with access to WMP Information Systems.

In this policy the term 'Individual' means police officers, special constables, police staff, volunteers, temporary and agency workers, staff employed by the Office of the Police and Crime Commissioner (OPCC), as well as third party staff or partner agencies who use WMP systems

2.0 PURPOSE OF POLICY

The purpose of the Acceptable Use Policy is to protect the confidentiality, integrity and availability of WMP information assets, whilst ensuring that all Individuals that use WMP systems understand and accept their personal responsibilities, in order to abide by the relevant legislation.

The Acceptable Use Policy has been developed in line with national policing standards and meets the WMP Service and Leadership Ethos of Simplicity, Standards and Service by ensuring all Individuals demonstrate the acceptable use of systems and information assets at all times.

The requirements within this policy have been set out in consideration with the Code of Ethics and our force's Vision and Values of Protecting People from Harm and taking ownership, whilst strengthening each individual policing priority by supporting the protection of the confidentiality, availability and integrity of our information assets.

3.0 IMPLICATIONS of the POLICY

The effective operation of this policy and associated procedures will support the delivery of effective policing services, assist in reducing costs incurred through unacceptable use and protect people from harm by ensuring that information is secure, accurate and available to the right people at the right time.

WMP is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to Individual who use Force Systems, who may be accountable for any breaches of Information Security for which they may be held responsible.

This policy and associated procedures support compliance with legal, national and best practice standards including, but not limited to;

- Freedom of Information Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990

- Official Secrets Act 1989
- HMG Security Policy Framework
- Governance and Information Risk Return
- ISO27001

There is a requirement for all Individuals with access to WMP systems to comply with this policy and its associated procedures, and where requested, to demonstrate such compliance. Failure to comply with the policy may be regarded as a disciplinary offence, and may be dealt with subject to misconduct proceedings. In serious cases, this may be treated as gross misconduct and may result in summary dismissal.

4.0 POLICY FRAMEWORK

General use of ICT Systems

Under no circumstances is any individual authorised to engage or encourage others to engage in any activity that is illegal under UK law.

Unacceptable Use

This includes, but is not limited to:

- An attempt to alter, disable, re-configure or bypass security measures on WMP IT systems, such as authentication, anti-virus protection and other protective measures.
- An attempt to install, remove or reconfigure hardware or software by unauthorised Individuals.
- Use of any other individuals' username, password or warrant/ ID card either with or without their consent.
- Permitting the use of a personal username, password or warrant/ ID card by another.
- Introduction of malicious programs onto force ICT systems, including, but not limited to, viruses and malware.
- Unauthorised sharing, copying or destruction of sensitive information.
- Sharing images, text, or material which is illegal, harassing, discriminating, indecent, obscene or likely to cause offence.
- Connecting non-force issued IT devices to WMP IT equipment or infrastructure via USB, serial, network, wireless (not including WMP public WIFI) or other means.
- Bringing the forces reputation into disrepute or conducting activity likely to impact or obstruct its visions, values and code of ethics.

Physical Security

Individuals are responsible for the security of mobile devices issued to them such as phones, laptops and removable media.

All laptops and tablets should be shut down when not in use or left unattended. When attended but not in use, password protection through screen lockout must be left enabled. No attempt to change these settings shall be made by an Individual.

Keys and door entry fobs which allow access to WMP premises must be given the same consideration as any other asset, in particular keys and door fobs / proximity cards must have no markings or key rings which indicate the premises that they are related to and must not be left unattended in vehicles.

Passwords

WMP's Passcode Procedure must be adhered to at all times, specifically Individuals must not share or disclose user account passwords to anyone, passwords must not be communicated, written down or stored insecurely.

Clear Desk and Clear Screen Procedure

In order to reduce the risk of unauthorised access or loss of information, WMP enforces a Clear Desk and Screen Procedure.

Bring Your Own Device

The use of personal equipment (commonly known as "Bring Your Own Device" or "BYOD") to store or process force information is not permitted.

The redirection of emails or any other force data to non-force supplied IT devices or user accounts is not acceptable.

Fixed IT Equipment

Individuals are not authorised to remove or relocate any IT equipment. This includes but is not limited to, desktop PCs, phones, printers, and associated cabling. If equipment needs to be relocated or stored due to a business change a request should be made to the IT Service Desk using MyBop.

Removable Media

WMP recognise the need to permit the storing and sharing of information using removable media, such as USB memory sticks and external hard disk drives. However, there are significant risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks along with details of why no practicable alternatives are available are to be demonstrated before approval is given.

Only WMP authorised devices with an IT asset marking shall be used when transferring data. These devices must only be connected to authorised equipment to reduce the likelihood of compromise to information and systems.

Individuals shall encrypt the device using force IT facilities before use and must securely return this to the IT department after use for the appropriate level of sanitisation to be carried out.

Information detailing the requirements for the use of removable media can be found in the Mobile Devices Procedure.

Use of Email

Internal and external email facilities are available to Individuals as required, subject to approval of local management. Emails containing sensitive information must only be sent to secure email addresses. Further guidance is available from the Information Classification Procedure, Use of Internet & Email Procedure and force Information Security Officer.

Force email services are restricted to business use only and forwarding of emails to external email accounts for a non-policing purpose is not permitted.

All emails will be stored electronically by the IT Department for a period of time and may be inspected by the force as per the Lawful Business Monitoring Policy. WMP reserves the right to copy, delete, disclose, or use email messages in any account without prior notice.

Use of the Internet

WMP will make Internet access available to Individuals for both business and limited personal use. Personal use of Internet access facilities is limited to non-work time only and will be subject to local business procedures.

Use of the Internet from WMP assets may be subject to monitoring, therefore any use cannot be assumed to be private.

Individuals must use Internet facilities in accordance with the Use of Internet & Email Procedure at all times.

Use of Social Media

WMP will communicate and engage with the general public and the communities it serves, via a range of social media. This shall be approved by local management or command teams and must be done in accordance with the force Social Media Policy.

Use of social media by Individuals, whether in a work related or a personal capacity, must not cause any reputational risk to the force, be of detriment to organisational activities or operations, and must be in line with all related procedures and guidance.

All social media messaging apps (e.g. WhatsApp) used for work purposes must be used on WMP devices not personal, and no Official WMP data is to be shared on such apps.

All social media apps/groups used for social purposes (including social networks with colleagues) must not be on work devices.

Mobile Device Usage

Requirements and guidance regarding the use of mobile devices such as laptops, phones, tablets, and storage devices, are covered in the Mobile Devices Procedure, which Individuals must read before using a device.

Requirements covering the acceptable use of mobile applications (or apps) are set out within the Use of Internet & Email Procedure.

Auditing of Access

Where possible WMP will record and monitor the use of all force information and communication systems in order to ensure the highest standards of professionalism and integrity alongside the prevention, investigation, and detection of criminal offences.

Individuals must be aware that there is no expectation of privacy when using force systems. WMP retains the right, with or without cause or notice, to access or monitor all IT information and data, including but not limited to:

- Email;
- Internet use;
- Instant messages; and
- Voice mail.

For more information, see the Lawful Business Monitoring Policy/ Procedure and Protective Monitoring Policy.

Incident Management

WMP recognise the need for an effective security incident management process.

Where Individuals suspect there has been either an actual or potential security incident, they must report this without delay by using the 'SIR1' form, following the Force Information Security Management Procedure on the Force Intranet and inform their line manager immediately.

The Individual's WMP or OPCC line manager must conduct a prompt and effective investigation with the support of the force Information Security Team and IT Security Officer. The aim of an investigation will be to aid in the recovery of data, reduce the risk of compromise to information assets and develop local force and local procedures to reduce the likelihood of reoccurrence of any future incidents

Associated Documents

- Clear Desk and Clear Screen Procedure
- Mobile Devices Procedure
- Use of Internet & Email Procedure
- Password Procedure
- Social Media Policy
- Physical Security Procedure
- Information Security Incident Management Procedure
- Off Site Security of Police Information and Equipment

- Lawful Business Monitoring Policy/ Procedure
- Protective Monitoring Policy

Documents are published to the Force Intranet and shall be made available to authorised third parties on request. Individuals must read and understand all policies which apply to their role.

<i>Business Lead/ Chief Officer Consulted</i>	<i>Date Consulted</i>
Simon Bennett/ Rachel Hartland-Lane	Sep 2022/ October 2022

5.0 DOCUMENT HISTORY

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
Aug 2020	D Archer	New West Mercia Policy v1.0	JNCC 10/11/2020
Sep 2022	D Archer	Mobile Device Usage – ACU changes v2.0	JNCC Exec Board 08/11/2022

6.0 CONSULTATION

The following have been identified as key stakeholders who will be part of the consultation exercise:

Head of Digital Services
 Head of IT Shared Services
 Head of Audit, Risk and Compliance
 Professional Standards Department
 Anti-Corruption Unit
 Information Security Manager
 Data and Records Manager
 Information Compliance Manager
 PSN Project Manager
 IT Shared Services Customer Services Manager
 Digital Services Technical Support Team Leader
 Digital Services Technical Support Level 3
 Critical Friends group
 UNISON
 West Mercia Police Federation

7.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.

8.0 DATA PROTECTION IMPACT ASSESSMENT

- Is a DPIA required? – **No**, as agreed by Audit, Risk and Compliance on 26/09/2022