WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Mobile Computing Policy**
POLICY REFERENCE NO:	**Inf/13**

Executive Summary.

In accordance with the HMG SPF Security Outcomes and the Cabinet Office Mobile Device Strategy, West Midlands Police will ensure that information risks associated with mobile computing are assessed, captured and remediated effectively, and that compliance controls for mobile computing in national Codes of Connection are complied with.

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

Intended Policy Audience.

This policy applies to every police officer, member of police staff, police community support officer, special constable, volunteer, contractor, and approved persons working for or on behalf of West Midlands Police.

Current Version And Effective Date.	**Version 0.3**	**15/10/2014**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Paul Richards, Information Security Officer**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**26/11/2014**	
Review Date	**26/11/2016**	
Protective Marking	**Not Protectively Marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- HMG Security Policy Framework (SPF);
- CESG IA Standards (IAS) and Good Practice Guides (GPG's);
- BS EN ISO27001 – Information Technology
- Security Assessment for Protectively Marked Assets (SAPMA)
- WMP Local Threat Assessment
- Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Diversity Vision Statement and Values

“Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values”

“All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay.”

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1. ABBREVIATIONS.

ACPO Association of Chief Police Officers
A/V Anti-Virus
ADS Accreditation Document Set (i.e. RMADS Risk Management Accreditation Document Set)
AO Accounting Officer (Chief Constable)
BC Basic Check
BCM Business Continuity Management
BCP Business Continuity Plan
BIA Business Impact Analysis
BS25999 Business Continuity Management - (BS 25999-1:2006) now ISO/IEC 22301:2012
CESG Communications-Electronics Security Group
CTC Counter Terrorism Check
CPU Central Processing Unit
DPA Data Protection Act 1998
DTI Department of Trade and Industry
HMG Her Majesty's Government
IAO Information Asset Owner
ICM Information Compliance Manager
InfoSec Information Security
ISF Information Security Forum
ISM Information Security Manager
ISO Information Security Officer (For the WMP Force)
ISO 22301 International Standards for Business Continuity Management - Requirements (ISO22301:2012)
ISO 27001 International Standard for Information Security Management System - Requirements (ISO27002:2005 contains the Implementation Guidance and Code of Practice)
IS Information Systems
ISP Information Security Policy
ISTU Information Systems Training Unit
ITIL Information Technology Infrastructure Library
LAN Local Area Network
NISCC National Infrastructure Security Co-ordination Centre
NPIRMT National Police Information Risk Management Team
PM Protectively Marked
RMADS Risk Management Accreditation Document Set
SC Security Check
SIRO Senior Information Risk Owner
SoA Statement of Applicability
SIIMN Strategic Information and Intelligence Management Board
SPF HMG Security Policy Framework
SyOPs Security Operating Procedures
SysOPs System Security Operating Procedures
System Information System
UNIRAS Unified Incident Reporting and Alerting Scheme.
UPS Uninterruptible Power
WMP West Midlands Police

2. TERMS AND DEFINITIONS.

Asset - An asset is something tangible or non-tangible which is of value to the organisation and needs to be protected, can be generally sub-divided into 'Primary Assets' and 'Supporting Assets'. **Primary Assets** are 'Processes' and 'Information Assets' used by, stored or communicated by the organisation. **Supporting Assets** are all other Hardware, Software, Networks, Utilities, Physical Premises, People and Organisational Structures that are present to make the use of the 'Primary Assets' possible;

Availability - Ensuring that authorised users have access to information and associated assets when required;

Confidentiality - Ensuring that information is accessible only to those authorised to have access;

Evaluation - The assessment of an IS system or product against defined criteria;

Identity and Access Management - In information systems, identity management is the management of the identity life cycle of entities (subjects or objects);

Information Asset - An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation;

Information Security Policy - The set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed;

Integrity - Safeguarding the accuracy and completeness of information and processing methods;

Risk - The likelihood of a threat occurring and being successful in exploiting vulnerability, and causing a breach of security;

Security - A combination of confidentiality, integrity and availability considerations;

Threat - The likelihood that an attacker will attempt, and has the capability, to exploit a vulnerability to breach security; and

Vulnerability - A feature of a system, which, if exploited by an attacker, would enable the attacker to breach security

3. INTRODUCTION.

Organisational mobility is an integral part of West Midlands Police strategy in exploiting and realising value from the disruptive potential of mobile platforms, applications and services as well as enabling novel work paradigms. A comprehensive policy is required to protect information assets and resources from known security threats associated with mobile devices, users and services, as well as retain the ability and authority to take appropriate measures that minimise the risk to our values, and operations.

4. MOBILE COMPUTING POLICY

4.1 Remote Environments

Formal documented standards and procedures should be in place to support Staff working in remote environments including public areas or from home that cover the following but not limited to:

- business area manager authorisation to work remotely
- security requirements and guidelines associated with remote working
- approved devices and locations for Staff working in remote environments
- standards for implementation, configuration, maintenance and security of computing devices and software located in remote environments
- protection against loss or theft

A risk assessment **must** be conducted prior to authorising work in remote environments to ensure such access does not expose business data to unacceptable risks.

Staff authorised to work in remote environments should be made aware of risks associated with remote working, informed of unapproved or unsafe locations for remote working, equipped with necessary tools and skills to perform required security tasks, and provided with adequate technical support and alternative working arrangements in the event of an emergency.

The controls framework **must** ensure computing devices used for working in remote environments are protected by appropriate physical and logical controls to reduce the risk of unauthorised access, loss or theft. The controls should include:

- tamper-proof asset tagging, and standard, technical configurations for corporate devices
- system management tools and utilities
- access control mechanisms to restrict access to the remote endpoint
- malware protection
- encryption solution to protect data at rest and in transit
- guidelines for equipment return and incident reporting

4.2 Mobile Endpoints

Formal documented standards and procedures should be in place to cover corporate mobile hardware and software deployment, architecture, configuration, management, monitoring and protection of sensitive information.

Corporate mobile devices **must** be provisioned with standard firmware and technical build configurations and subject to system hardening in accordance with their risk profile, platform features and capabilities, and requirements of the control framework.

The controls framework should ensure that corporate mobile endpoints are consistently protected against security threats in accordance with the Cabinet Office Mobile Device strategy by enabling:

- centralised management and control using approved system management tools to facilitate routine maintenance and support procedures

- password, sign-on and access control mechanisms that restrict access to the device and from the device
- current malware and intrusion protection, removable device control and data leakage protection

The controls framework **must** safeguard sensitive information stored on corporate mobile endpoints based on an assessment of the platform's capabilities, inherent risk exposures and required degree of protection. The controls should, as appropriate for the technology, include:

- full disk encryption for internal hard disks
- file-based encryption software to safeguard individual files and folders
- enforced encryption over data copied to portable storage and flash memory cards
- sandboxing or other secure containerization solutions

Corporate mobile endpoints **must** be enrolled within the enterprise mobile device management platform for consistent enforcement of security policies and standards, and on-going device management and monitoring, in accordance with the controls framework.

The controls framework **must** enforce adequate protection for sensitive information on corporate mobile endpoints used to access business applications, by preventing or reducing the amount of application information being stored on the device and protecting application information when it is stored on the endpoint.

Mobile endpoint **must** be configured to log important events including a potential compromise of or reduction in the required security level of the device.

Mobile endpoints should enforce controls that:

- restrict copying or transfer of sensitive information only to authorised portable storage devices
- prevent, detect and log use of or connection to unauthorised portable storage devices
- monitor information copied to portable storage devices to help detect unauthorised transfers
- address threats from connecting to unauthorised or untrusted networks and computing devices

Mobile endpoints accessing the WMP network from remote environments **must** be configured to:

- establish a secure network connection between the endpoint and the corporate network
- employ strong user and device authentication
- prevent access to unprotected networks while connected to the corporate network

Mobile endpoints requiring access to the Internet should be subject to security controls that enforce authenticated access to the Internet, restrict access to only authorised web sites, inspect web traffic for malware and other attacks, and log user activity.

4.3 Portable Storage Devices

The controls framework **must** ensure the use of portable storage devices is:

- risk assessed and authorised based on the results of the risk assessment
- restricted to approved device types
- adequately protected against relevant security threats
- logged and regularly monitored

The controls framework should ensure data transfers to portable storage devices are encrypted using approved cryptographic standards and logged to facilitate periodic review.

Staff should be made aware of the risks associated with the use of portable storage devices and provided working guidelines that cover the following:

- secure storage of devices when not in use
- periodic review of content on the devices
- secure disposal of devices and destruction of information held on the devices
- returning the devices when no longer required and reporting any incident of loss or theft
- prohibiting data transfers to personal devices, sharing of the devices or disclosing passwords for accessing information on them to unauthorised individuals
- corporate ownership of all information held on the device and organisational right to recover information held on them

4.4 Non Conformance and Exceptions

Non-conformance to this policy must be reported to the Information Security Officer (ISO). The ISO must approve, track and report all exceptions to this policy in accordance with a formal documented process. The process should include a method for escalating significant exceptions that may breach a documented level of business risk tolerance, to appropriate boards and committees in accordance with established governance procedures for review and mitigation or formal risk acceptance

5. UNDERPINNING POLICIES AND PROCEDURES

To support the overarching IA Risk Management policy the following policies will be maintained by the force –

1. Physical security policy;
2. Force Information Security Policy;
3. Information Management Policy;
4. Information Security Incident Management Policy;
5. Information Services Risk Register;
6. West Midlands Police Risk Appetite Statement;

6. EQUALITY IMPACT ASSESSMENT (EQIA).

The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how WMP has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

7. HUMAN RIGHTS.

This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

8. FREEDOM OF INFORMATION (FOI).

Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.2 of this policy has been GPMS marked as Not Protectively Marked.

Public disclosure does not automatically apply to supporting Force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number
N/A		

9. TRAINING.

This policy reflects best practice within ICT and IM and does not require a training element

10. PROMOTION / DISTRIBUTION & MARKETING.

The following methods will be adopted to ensure full knowledge of the Policy:

- Newsbeat
- Intranet
- Posters
- Policy Portal

11. REVIEW.

The policy business owner Information Management, maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted by the date shown as indicated on the first page.

Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

CHIEF CONSTABLE

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	21/03/2014	Initial Draft	Del Brazil, Advent-IM
0.2	21/07/2014	Amended Draft	Paul Richards
0.3	15/10/2014	Amended Draft	Stephen Laishley
0.3	15/10/2014	Amended formatting	56408 Couchman
0.3	27/11/2014	Policy approved and implemented	56408 Couchman