WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**SECURITY OF REMOVABLE MEDIA**
POLICY REFERENCE NO:	**Inf/29**

Executive Summary.

West Midlands Police (WMP) will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official WMP business.

***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 0.2**	**9 Feb 2015**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Dave Holden**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**20/04/2015**	
Review Date	**20/04/2017**	
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 A.9 – Information Technology
- Security Assessment for Protectively Marked Assets (SAPMA)
- WMP Local Threat Assessment
- WMP Information Security Policy
- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*

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. INTRODUCTION 5
2. SECURITY OF REMOVABLE POLICY 6
3 APPLYING THE POLICY 7
4 DEFINITION OF MEDIA 9
5. UNDERPINNING POLICIES AND PROCEDURES 10
6. EQUALITY IMPACT ASSESSMENT (EQIA) 10
7. HUMAN RIGHTS. 10
8. FREEDOM OF INFORMATION (FOI) 10
9. TRAINING. 11
10. PROMOTION / DISTRIBUTION & MARKETING 11
11. REVIEW. 11
12. VERSION HISTORY 12

1. INTRODUCTION

1.1 Purpose

1.1.1 This document states the Removable Media policy for WMP. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

1.1.2 This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of WMP's computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

1.2 Key Messages

1.2.1 The key messages within this policy are summarised below:-

- It is general WMP policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by WMP **must not** be used.
- All data stored on removable media devices **must** only be on encrypted devices. From time to time explicit permission to use non-encrypted devices may be granted in cases where encryption prevents lawful police duties such as transferring information to the Courts or CPS. Additionally non-sensitive data such as training materials may with explicit permission be transferred using unencrypted media. In these cases individuals will sign an additional security operating procedure.
- Damaged or faulty removable media devices must not be used.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

- Removable media devices that are no longer required, or have become damaged, must be returned to ICT to be disposed of securely to avoid data leakage.

1.3 Scope

1.3.1 This policy applies to all Departments, Partners and Employees of the West Midlands Police Force, contractual third parties and agents who have access to WMP information, information systems or IT equipment and intend to store any information on removable media devices.

2. SECURITY OF REMOVABLE POLICY

2.1 Statement

2.1.1 WMP recognises that there are risks associated with users accessing and handling information in order to conduct official WMP business. Information is used throughout the WMP and sometimes shared with external organisations and applicants. Securing sensitive information is of paramount importance – particularly in relation to the WMP's need to protect data in line with the requirements of the Data Protection Act 1998.

2.1.2 Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the WMP. It is therefore essential for the continued operation of the WMP that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the WMP's needs.

2.1.3 This policy aims to mitigate the following risks:

- Disclosure of protectively marked and organisation information assets as a consequence of loss, theft or careless use of removable media devices.
- Harm to investigations or individuals if police information whether personal or tactical is obtained and misused;
- Contamination of WMP networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the WMP or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the WMP or individuals as a result of information loss or misuse.
- WMP reputational damage as a result of information loss or misuse.

2.1.4 Non-compliance with this policy could have a significant effect on the efficient operation of the WMP and may result in an inability to provide necessary protection and services to our partners and the communities we serve.

2.2 Policy Compliance

2.2.1 Whilst respecting the privacy of authorised users, WMP maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of removable media by authorised users to ensure adherence to this Policy.

2.2.2 Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of items from removable media does not necessarily result in permanent deletion.

2.2.3 In addition to routine monitoring and audits, where a manager suspects that the removable media is being abused or misused by a user, they should report it as a security incident following the procedure documented on the intranet.

2.2.4 In addition WMP will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for information.

2.2.5 If any user is found to have breached this policy, they may be subject to WMP's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

2.2.6 If you do not understand the implications of this policy or how it may apply to you, seek advice from your line management, the information security team or ICT.

3 APPLYING THE POLICY

3.1 Restricted Access to Removable Media

3.1.1 It is WMP's policy to discourage the use of removable media as far as reasonably practicable. Where there is no practicable alternative then removable media may be used only when a valid business case is provided and agreed by the appropriate Departmental Information Management representative. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

3.1.2 Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

3.2 Procurement of Removable Media

3.2.1 All USB memory sticks and external hard drive devices must only be purchased through WMP ICT. Non-WMP owned removable media devices of any type must not be used to store any information used to conduct official WMP business, and must not be used with any WMP owned or leased IT equipment.

3.2.2 The only equipment and media that should be used to connect to WMP equipment or the WMP network is equipment and media that has been purchased by WMP and approved by WMP ICT.

3.3 Security of Data

3.3.1 In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

3.3.2 Each individual is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

3.3.3 All data stored on removable media devices must be on encrypted devices. From time to time explicit permission to use non-encrypted devices may be granted in cases where encryption prevents lawful police duties such as transferring information to the Courts or CPS. Additionally non-sensitive data such as training materials may with explicit permission be transferred using unencrypted media. In these cases individuals will sign an additional security operating procedure.

3.4 Incident Management

3.4.1 It is the duty of all users to immediately report any actual or suspected breaches in information security to their line manager and to the security teams using the Information Security Incident form on the intranet..

3.5 Third Party Access to WMP Information

3.5.1 No third party (external contractors, partners, agents, the public or non-employee parties) may extract information from WMP's network information repository or IT equipment and place on a removable media device without explicit agreement by the relevant Information Asset Owner in consultation with the Information Security team. Should third parties be allowed access to WMP information then all the considerations of this policy apply to their storing and transferring of the data.

3.6 Preventing Information Security Incidents

3.6.1 Damaged or faulty removable media devices must not be used. It is the duty of all users to stop using removable media when it is damaged.

3.6.2 Virus and malware checking software approved by WMP must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned before the media is loaded on to the receiving machine.

3.6.3 Secure means of transit and storage must be agreed, documented and implemented.

3.7 Disposing of Removable Media Devices

3.7.1 Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to WMP ICT for secure disposal.

3.7.2 For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact WMP ICT.

3.8 User Responsibility

3.8.1 All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with WMP equipment or the network or to hold information used to conduct official WMP business must only be purchased and installed by the ICT team. Any removable media device that has not been supplied by the ICT must not be used.

- All data stored on removable media devices must only be stored on encrypted devices supplied through ICT.

- Virus and malware checking software must be used when the removable media device is connected to a machine.

- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.

- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- A record of the information placed onto any removable media device must be kept by the user and be available to Professional Standards, Information Security personnel or Appropriate Authority in the event of any actual or suspected breach in information security.

- Information held on a removable media device must be kept to a minimum.

3.8.2 For advice or assistance on how to securely use removable media devices, or for further advice or clarification on any part of this policy, please contact Information Security from the Intranet security pages.

3.9 Policy Compliance

3.9.1 Whilst respecting the privacy of authorised users, WMP maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of removable media by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of items from removable media does not necessarily result in permanent deletion.

4 DEFINITION OF MEDIA

4.1.1 This policy should be adhered to at all times, but specifically whenever any user intends to store information used by the West Midlands Police to conduct official business on removable media devices.

4.1.2 Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).

- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

5. UNDERPINNING POLICIES AND PROCEDURES

5.1. To support the overarching Security of Removable Media policy the following policies will be maintained by the force –

- Force Information Security Policy;
- Information Management Policy;
- Information Security Incident Management Policy;
- Asset Management Policy;
- Information Classification Policy;

6. EQUALITY IMPACT ASSESSMENT (EQIA).

6.1. 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 West Midlands Police 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.

7.1. 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 West Midlands Police (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

8. FREEDOM OF INFORMATION (FOI).

8.1. Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.1 of this policy has been GPMS marked as Not Protectively Marked.

8.2. 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.

9.1. There is no specific training for West Midlands Police personnel; however those individuals with a specific involvement in Security of Removable Media will have the relevant training courses detailed within their job specifications.

10. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

10.2. No uncontrolled printed versions of this document are to be made without the authorisation of the document owner.

11. REVIEW.

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

11.2. 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.

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

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

11.5. 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	27 January 2014	Initial document	Dave Holden
0.2	9 February 2014	Some amendments to tie up with force policy.	Kate Jeffries
0.2	27/04/2015	Chief Constable has signed and approved police – policy is now live	56408 Couchman