WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Cryptographic Policy**
POLICY REFERENCE NO:	**Inf/26**

Executive Summary.

The purpose of this Policy is to establish rules for the encryption of classified data from West Midlands Police systems to other location and media.

***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 0.1**	**2 March 15**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Tom King – Information Security Officer**	
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 ISO 27001:20013 – 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. INTRODUCTION.

1.1. Information security requires the participation and support from all WMP Employees with access to information assets. It is the responsibility of all Employees to help ensure that all information assets are kept secure but available on a need-to-know basis. Encryption techniques must be employed when data of a PROTECT or RESTRICTED nature is transferred electronically. This Policy must be read in consultation with the Information Classification Policy; and

1.2. The storage, disclosure and destruction of cryptographic keys must at all times be managed by authorised employees in line with all relevant agreements, legislation, regulations and industry best practice.

2. CRYPTOGRAPHIC POLICY

2.1 Non Conformance and Exceptions

2.1.1 All laptops must have full disk encryption installed, and when connected remotely, must connect via encrypted VPNs.

2.2 Mobile and PDA Devices

2.2.1 All Mobile and PDA devices must be configured in accordance with the latest procedures for administers and users. They must be configured using SSL VPN encryption.

2.3 Data in Transit

Network Connections and Remote Access

2.3.1 All network connections that conduit protectively marked information between sites must be connected using encrypted VPN devices.

2.3.2 Remote access must only be via an encrypted link;

Email

2.3.4 RESTRICTED data must not be transmitted externally in attachments to emails without first being given password protection. It is at the discretion of the sender as to whether PROTECT information requires encryption.

2.3.5 Passwords must be advised to the intended recipient by means other than email (e.g. by telephone or text message)

USB

2.3.6 Data stored on corporately owned and encrypted USB media sticks may be carried by hand or sent via standard surface mail postal services.

CD/DVD

2.3.7 CD/DVDs are not permitted on the force network except those which are used to carry non-sensitive information (such as training material). In some controlled circumstances where encryption cannot be supported (such as CPS files) additional procedures will be employed to protect and control unencrypted media.

Physical Security

2.3.8 Employees are responsible for the physical security of laptops, mobile phones and other devices issued to them. Loss of a company mobile phone, laptop computer or other portable device must be reported to the Line Manager and to Information Security (using the on-line security incident reporting form)

2.4 Non Conformance and Exceptions

2.4.1 Non-conformance to this policy must be reported to the relevant team. Information Security, Risk and Privacy 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

3. UNDERPINNING POLICIES AND PROCEDURES

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

1. Information Security Policy;
2. Information Services Risk Register;
3. West Midlands Police Risk Appetite Statement;
4. Information Risk Management Policy

4. EQUALITY IMPACT ASSESSMENT (EQIA).

4.1 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.

5. HUMAN RIGHTS.

5.1 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.

6. FREEDOM OF INFORMATION (FOI).

6.1 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.

6.2 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		

7. TRAINING.

7.1 There is no specific training for West Midlands Police personnel; however those individuals with a specific involvement in systems management will have the relevant training courses detailed within their job specifications.

8. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

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

9. REVIEW.

9.1 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.

9.2 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.

9.3 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.

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

9.5 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.

10. PROFESSIONAL STANDARDS OF BEHAVIOUR.

10.1 All staff are reminded that it is their personal responsibility to protect the data held within police systems, in line with force policy and legislation, and to ensure that it is only used for a clearly defined policing purpose. Any unauthorised access to, or disclosure of data for a non-policing purpose could lead to criminal or disciplinary proceedings

CHIEF CONSTABLE

13. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	2 March 15	Initial Draft	Tom King/Stephen Laishley
0.1	27/04/2015	Policy signed off by CC – policy now live.	56408 Couchman