WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Information Classification Policy - GPMS**
POLICY REFERENCE NO:	**Inf/19**

Executive Summary

In accordance with the HMG SPF Risk Management West Midlands Police will ensure that appropriate security measures are implemented and managed to control access to information assets and reduce the risks associated with unauthorised system access and information disclosure.

***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**	**14/01/2015**
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	**10/02/2015**	
Review Date	**10/02/2017**	
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 ISO27001:2013 – 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 5
2. INFORMATION CLASSIFICATION POLICY 5
The Aim of the Policy 5
General Principles of the Policy 6
Protective Marking Criteria 7
Descriptors 9
Baseline Measures 10
Disclosure of Protectively Marked Information 11
Implementation 11
3. UNDERPINNING POLICIES AND PROCEDURES 12
4. EQUALITY IMPACT ASSESSMENT (EQIA). 12
5. HUMAN RIGHTS. 12
6. FREEDOM OF INFORMATION (FOI). 12
7. TRAINING. 13
8. PROMOTION / DISTRIBUTION & MARKETING. 13
9. REVIEW. 13
10. VERSION HISTORY 14
APPENDIX A 14

1. INTRODUCTION

1.1. This policy applies to all authorised users of West Midlands Police Information and is therefore applicable to all staff, whether permanent or temporary and to any third party contractors or partners who have access to such information.

1.2. This is achieved by a risk assessed approach and by adopting measures that preserve:

- Confidentiality – ensuring that information/intelligence is accessible only to those authorised to have access and protecting assets against unauthorised disclosure.
- Integrity – safeguarding the accuracy and completeness of information and processing methods, and protecting assets from unauthorised or accidental modification.
- Availability – ensuring that authorised users have access to information and associated assets when required to pursue West Midlands Police objectives.

1.3. This policy is part of a suite of guidance that links to the Information Assurance Strategy and Force Security Policy. As such users need to take cognisance of the national Code and Guidance related to the Management of Police Information.

2. INFORMATION CLASSIFICATION POLICY

The Aim of the Policy

2.1. To ensure our legal use of information/intelligence is balanced with the needs of information/intelligence security and to ensure that the force complies with the Association of Chief Police Officers (ACPO) Council decision to adopt the Government Protected Marking Scheme and reflects relevant considerations regarding the Code and Guidance of the Management of Police Information.

2.2. The protective-marking scheme is a method for creating a common standard within the police service for the valuation and protection of the information assets available within the service.

2.3. The purpose of this document is to implement the necessary controls contained within the Security Policy Framework in the context of the business requirements of West Midlands Police.

2.4. The policy applies to the protection of all information (manual or electronic). By protectively marking our information assets the sensitivity of the material is assessed by determining the likely consequences of that material being compromised.

This policy will enable the Force to:

2.5. Apply appropriate protective measures to our material according to the likely consequences of its compromise;

- have a common understanding with government departments and other police forces about the measures required to protect shared material in matters such as organised crime, drugs trafficking and intelligence;
- have a common understanding with other agencies about measures needed to protect any material that we pass to them; and
- have a common understanding with contractors and suppliers about measures needed to protect any material that we pass to them in compliance with any relevant protocols

General Principles of the Policy

2.8. The policy applies to all Police Officers, Police Staff, Partnership Staff and all personnel contracted to work for West Midlands Police, Special Constables, Volunteers, temporary personnel and trusted employees from agencies and organisations who by the nature of their role require access to West Midlands Police information systems.

2.9. The majority of information held within the police force is sensitive and requires a protective marking value. The marking, an information asset requires, will be ascertained by identifying what would happen if the information was to be compromised.

2.10. Consideration has to be given to the impact upon an individual, the Force, major organisations and national security.

2.11. The effectiveness of this system is closely linked to the “Need to Know” approach to information management and to the Force Vetting Policy. Fundamental to the principles of protective marking is the fact that “Need to Know” has dual interpretation restricting information to those who have a need for such information and ensuring that those who do require that information are not prevented from receiving it.

2.12. Protective Marking is one of a series of controls West Midlands Police will utilise in order to protect its information assets. The policy and procedures are derived from the Security Policy Framework.

2.13. This policy provides the appropriate controls for the marking, handling, movement, storage and disposal of sensitive material.

“Need to Know”

2.14. One of the major principles of the Protective Marking scheme is the “Need to Know” principle. This principle states that only individuals with a legitimate reason for obtaining information are able to do so. For example, only those individuals directly involved with an investigation into serious crime have the right to access information held relating to that crime. Other members of the same Force / Station have no legitimate need to view the information. “Need to Know” also means there is a requirement to inform those with an operational or business need to access the information.

2.15. In order for Protective Marking to be effectively implemented, it is important that staff understand and view the principles contained within the “Need to Know” doctrine as an enabling mechanism.

2.16. The purpose of this principle is to allow members of staff to provide and receive information that is relevant and helpful to the Force’s specific business needs and those of the proposed recipient of the information.

2.17. It introduces a simple decision making process when members of staff are in a position to disclose information, by asking themselves whether the recipient needs to know, for their business purposes:

- All of the information
- Some of the information, or
- Any of the information.

2.18. The application of this principle will enable members of staff to supply and receive information in pursuance of Police business. This ensures all the disclosures of information either within the Force, or externally to other partnership and law enforcement agencies, will meet the requirements set by Legislation and Force Policy.

Protective Marking Criteria

2.19. All information assets will both not be protectively marked (and thus unprotected) or utilise one of the five classifications of:

- PROTECT, Impact levels 1 and 2
- RESTRICTED, Impact level 3
- CONFIDENTIAL, Impact level 4
- SECRET, Impact level 5
- TOP SECRET, Impact level 6

2.20. In addition where an information asset requires special handling instructions an approved descriptor may be attached to that asset, for example: RESTRICTED-MEDICAL; CONFIDENTIAL-INTEL; CONFIDENTIAL-OPERATION LITOTES; SECRET-CHIS. (See below).

2.21. Information that either has been obtained from the public domain, or due to its content may be disclosed to the public domain (e.g. contents do not fit into the above four categories), will be identified as “Not Protectively Marked”

PROTECT - The compromise of assets marked PROTECT would be likely to:

Impact level 1

- No impact on life and safety
- Minor disruption to emergency service activities that requires reprioritisation at local (station) level to meet expected levels of service
- No impact on crime fighting
- No impact on judicial proceedings

Impact level 2

- Inconvenience or cause discomfort to an individual
- Minor disruption to emergency service activities that requires reprioritisation at area / divisional level to meet expected levels of service
- Minor failure in local Magistrates Courts
- PROTECT is not a national security protective marking and the policy relating to the use of RESTRICTED remains unchanged.
- PROTECT is not to be used for operational issues.
- PROTECT must be accompanied by a Descriptor, (e.g. PROTECT – STAFF).

RESTRICTED - The compromise of assets marked RESTRICTED would be likely to:

- Adversely affect diplomatic relations
- Cause substantial distress to individuals
- Make it more difficult to maintain the operational effectiveness or security of the UK or allied Forces.
- Prejudice the investigation or facilitate the commission of crime
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Impede the effective development or operation of government policies
- Breach statutory restrictions on disclosure of information (does not include the Data Protection Act 1998, where non-sensitive personal information is involved)
- Disadvantage government in commercial or policy negotiations with others
- Undermine the proper management of the public sector and its operations

CONFIDENTIAL – The compromise of assets marked CONFIDENTIAL would be likely to:

- Materially damage diplomatic relations, that is, cause formal protest or other sanctions.
- Prejudice individual security or liberty.
- Cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations.
- Work substantially against national finances or economic and commercial interests.
- Substantially undermine the financial viability of major organisations.
- Impede the investigation or facilitate the commission of serious crime (Serious crime as defined by the Regulation of Investigatory Powers Act 2000 see Sect. 81(3)).
- Seriously impede the development or operation of major government policies.
- Shut down or otherwise substantially disrupt significant national operations.

SECRET - The compromise of assets marked SECRET would be likely to:

- Raise international tension.
- Seriously damage relations with friendly governments.
- Threaten life directly or seriously prejudice public order or individual security or liberty.
- Cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations.
- Cause substantial material damage to national finances or economic and commercial interests

TOP SECRET - The compromise of assets marked TOP SECRET would be likely to:

- Threaten directly the internal stability of the UK or friendly countries.
- Lead directly to widespread loss of life.
- Cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations.
- Cause exceptionally grave damage to relations with friendly governments.
- Cause severe long-term damage to the UK economy.

Descriptors

2.22. In addition to the use of a protective-marking classification it is also possible to further label assets with a descriptor. A descriptor is applied if the asset may require specific handling considerations. This not only helps in the handling of the asset BUT also enhances the users' ability to assess the necessity of applying the "Need to Know" principle.

2.23. A descriptor is not essential but may be added to help indicate the nature of the sensitivity and the groups of people who need access. The following descriptors, which are not exhaustive, may be used.

2.24. Whilst the Manual of Protective Security does not mandate specific descriptors, there are certain descriptors used throughout the public sector, which should be considered for the purpose of consistency. The following are commonly used descriptors, which should be considered where appropriate.

- APPOINTMENTS - concerning actual or potential appointments that have not yet been announced;
- CHIS (Covert Human Intelligence Source) - regarding informants and their handling. Any informant related information shall be treated at as baseline CONFIDENTIAL with the appropriate handling procedures. Information that identifies an informant may require marking at SECRET
- COMMERCIAL - relating to a commercial establishment's processes or affairs;
- CONTRACTS - concerning tenders under consideration;
- CRIME - concerning crime;
- HONOURS - recognition given for exceptional achievements.,
- INTEL - criminal intelligence.,
- INVESTIGATIONS - concerning investigations into disciplinary or criminal matters;
- MANAGEMENT -policy and planning affecting the interests of groups of staff;

- MEDICAL - medical reports and records and material relating to staff;
- OPERATION 'NAME' – to restrict material to those involved in the operation
- PERSONAL - material intended for the person to whom it is addressed-;
- POLICY - proposals for new or changed government or Force policy before publication;
- PRIVATE – for information collected through electronic government services or provided to the public and agencies and relating to the individual or agencies
- STAFF - concerning references to named or identifiable staff or personal confidences entrusted by staff to management.
- VISITS - concerning details of visits by, for example, royalty and ministers of state.

2.25. With the exception of PERSONAL and PRIVATE, which may be used by them, the above descriptors may only be used in conjunction with a Protective Marking, e.g. RESTRICTED – MEDICAL. This does not relate to the title of any file or folder.

2.26. Information sent to either an individual member of the public, or an organisation that does not subscribe to the Manual of Protective Security will be marked with a descriptor of PRIVATE. In order to minimise disruption to the Force, information sent to Partnership Agencies will retain the relevant Protective Marking. Guidance will be provided to as required to Partnership Agencies as to the handling requirements of such information.

Baseline Measures

2.27. Information assets marked as SECRET and TOP SECRET will routinely only be stored by the WM CTU.

2.28. No information or data marked above RESTRICTED should be stored or processed on the Force Network.

2.29. The key to successful use of Protective Marking is consistent marking, which requires a common-sense approach by the originator of the material. If material is originated which requires a PROTECT, RESTRICTED or CONFIDENTIAL marking, it must be marked at the time of origin. Some West Midlands Police systems are not GPMS compliant and do not contain a GPMS marking on any printed material. It is the responsibility of any persons printing documents to ensure that the correct GPMS marking is written clearly or stamped on the document.

2.30. The protective marking must be conspicuous so that the value of the material is clearly conveyed to those who need to know to ensure all those who may handle it are aware of the level of protection required. The marking will be at the top and bottom of every page (within the 'Header' and 'Footer') in capitals and in black font.

2.31. The protective marking of any material must not be downgraded without referring back to the originator.

2.32. Increasing the protective marking of a document or a file containing a number of documents will be at the discretion of the individual handling it, subject to the principles in this policy. This will normally be achieved by placing it within a folder indicating the higher level of security, previous routing will be retained with the folder.

2.33. Care should be taken when handling information from agencies that do not mark their information assets. It is recommended that any information containing details of either a sensitive and/or personal nature should be treated as RESTRICTED. This includes information bearing the descriptor of PRIVATE. Old material bearing any form of IN CONFIDENCE marking should be treated as if it were at least RESTRICTED.

2.34. Protectively marked material must only be produced, handled and reproduced by persons with authorised access to it. The “Need To Know” principle must be applied, limiting material to those with a genuine “Need to Know” in order to discharge their duties. In particular, careful thought should be given to limiting the production of copies.

2.35. CONFIDENTIAL material should be regularly reviewed to consider the issue of protective marking with a view to downgrading or disposal in accordance with the Force policy on the retention of information.

2.36. Any protectively marked document should be stored within the appropriate secure environment when it is not being worked upon.

Disclosure of Protectively Marked Information

2.37. Protective Marking will assist in the protection of sensitive material, but the absence of a protective marking does not necessarily mean that the material may be made freely available. Conversely, the presence of a protective marking does not mean the material should not be disclosed in appropriate circumstances (for example, release of personal data to data subjects under the provisions of the Data Protection Act or to other bodies under the provisions of the Crime and Disorder Act).

2.38. Some West Midlands Police systems are not GPMS compliant and do not contain a GPMS marking on any printed material. It is the responsibility of any persons disclosing or sharing information to ensure that the correct GPMS marking is written clearly or stamped on any such material.

2.39. Protective Marking does not mean that the material can be withheld under Freedom of Information legislation unless an exemption applies. Any disclosure of information must be in accordance with current Force Policy.

GUIDANCE – See Appendix A

2.40. The Handling Protectively Marked Material – Guide for Police Personnel contains advice on the storage, transmission and destruction of protectively marked assets.

Implementation

2.42. The implementation of Protective Marking requires the Force to undertake a cultural change in its understanding and methods for the marking, handling, movement, storage and disposal of ‘sensitive’ material.

2.43. A full ‘clear desk’ policy must be the aspiration of this policy. This will have to be an on-going consideration as office accommodation is updated and budget considerations need to be coordinated to meet the above overall timescales.

2.44. Any further detailed advice on Protective Marking and in relation to the Security Policy Framework may be sought from the Force Information Security Officer.

3. UNDERPINNING POLICIES AND PROCEDURES

3.1. To support the overarching Information Classification policy the following policies will be maintained by the force –

1. Physical security policy;
2. Vetting\personnel policy;
3. Force Information Security Policy;
4. Information Management Policy;
5. Password Management Policy;
6. Information Security Incident Management Policy;
7. Clear Desk & Screen Policy;
8. Information Services Risk Register;
9. West Midlands Police Risk Appetite Statement;

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 0.2 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 Information Classification 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.

CHIEF CONSTABLE

10. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	30 Dec 2014	Initial Draft	Tom King/Stephen Laishley
0.2	14 Jan 2015	Amended Version	Tom King/Stephen Laishley
0.2	10/02/2015	Policy Approved- Added CC signature and policy reference no	56408 Couchman

APPENDIX A

ACPO Guidance Document:
Handling Protectively Marked Material, A Guide for Police Personnel