WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Digital Forensic Readiness**
POLICY REFERENCE NO:	**Inf/30**

Executive Summary.

West Midlands Police (WMP) will ensure the there is an ability within the organisation to make use of digital evidence when required. The policy's aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.

Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence related monitoring and collection processes and capabilities, storage requirements and costs

***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 0.4 (draft)**	**15 Apr 2015**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Tom King**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**27/05/2015**	
Review Date	**27/05/2017**	
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

1.1 Purpose

1.1.1 Forensic readiness is a key component of West Midlands Police (WMP) information risk. This will maximise WMP's potential to use digital evidence whilst minimising the cost of an investigation. This directive reflects the high level of importance placed upon minimising the impacts of information security incidents and safeguarding the interests of the public, staff and the organisation.

1.1.2 The aim of the forensics readiness policy is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required from a formal dispute or legal process. The policy may include evidence in the form of log files, emails, back up data, mobile computing, network, removable media and others that may be collected in advance of an event or dispute occurring.

1.2 Key Messages

1.2.1 The Digital Forensic Readiness Policy is a part of WMP's framework of Information Security Policies. It is designed to help protect the information assets of WMP through the application of best practice in IT Forensics and to minimise the costs of an investigation.
IT Forensics is the ability to detect and react to types of security incidents that require the collection, storage, analysis and preparation of digital evidence that may be required in legal or disciplinary proceedings. The Forensic Readiness Policy describes WMP's current capability to conduct an examination in a consistent, legal fashion and to ensure the admissibility of evidence relating to an incident. It covers both the proactive forensic monitoring of targeted systems and the reactive investigation of an unforeseen incident.

Such incidents will include, but are not limited to:

• Inappropriate use of equipment;

• Use of another user's logon credentials;

• Any attempt to circumnavigate existing or proposed security controls; and

• Any attempt to use police systems or information for corrupt or criminal reasons.

1.3 Scope

1.3.1 This policy supports the objectives of WMP's Information Security Management Strategy and applies to all staff, contactors, locums, agency workers, volunteers and third party agents with access to ICT services provided by or on behalf of the WMP.

The policy applies to all Trust Information, Communication and Technology (ICT) equipment, networks, software and information assets.

.

2. DIGITAL FORENSIC READINESS POLICY

2.1 Statement

2.1.1 The Board recognises that the aim of forensics is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for formal dispute or legal process. In this context, Forensics may include evidence in the form of log files, emails, back-up data, removable media, portable computers, network and telephone records amongst others that may be collected in advance of an event or dispute occurring.

2.1.2 Digital systems and distributed computing offer WMP great advantages in terms of efficiencies and cost saving. However our increased reliance upon these systems has proportionally increased this risk vector, something the adoption of good practice and controls can help to reduce or eliminate. However, it is necessary, as part of incident response, to have the ability to collect and analyse data held on a variety of electronic devices or storage media that may be used as evidence in some future investigation.

2.1.3 Proactive forensic monitoring comprises of those systems and practices in place at WMP for monitoring computers, users, groups or systems. Examples of such practices include, but are not limited to: computer security logs, email logs, internet traffic monitoring and telephone exchange logs.

2.1.4 Any forensic investigation will begin only at the request of a Ch Insp or higher from the Professional Standards Department (PSD). PSD will review the alleged incident and decide whether the investigation will be led by local management or from within PSD. At this point the investigating officer will be agreed and in the case of local management should be the person already nominated as the Appropriate Authority for that section.

2.1.5 Any tasks in a forensic investigation will generally be conducted by a suitably trained WMP individual. However, the SIRO may in some cases choose to engage the services of a suitably qualified third party.

2.1.6 All evidence provided as part of an investigation must be recorded and securely stored in such a way as to maintain its integrity until such time as the case, any hearings and appeals have concluded.

2.1.7 Any investigation which presents a suspicion of criminal activity should be reported to the Head of Information Management for logging and escalating as appropriate.

3. RESPONSIBILITIES

3.1 Senior Information Risk Officer (SIRO)

3.1.1 The SIRO will –

- Report serious cases to the Command Team as appropriate;
- Ensure adequate resources are made available to complete the necessary tasks;
- Where necessary directs senior management on the need to change Information Security practices to comply with legislation, regulations and any improvements identified as a result of the investigation.

3.2 Head of Professional Standards

3.2.1 The Head of PSD will directly or through senior PSD colleagues –

- Ensure that all reported incidents are reviewed and the correct level of investigation agreed – either PSD or local management;
- Appoint an investigative lead;
- Approve (or otherwise) use of forensic investigation; and
- Report the incident to the Head of Information Management.

3.3 Head of Information Management

3.3.1 The Head of IM is responsible for –

- Coordinating the development and maintenance of the force's forensic policy procedures and standards;
- Advising the Strategic Information Management Board (SIMB) and therefore the SIRO on forensic readiness planning and providing periodic reports and briefings on progress;
- Reporting issues to the Information Commissioner's Office when appropriate; and
- Having oversight of all investigations and ensuring appropriate records are kept;

3.4 Information Asset Owners (IAOs)

3.4.1 Ensures that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned 'ownership'. Goals for forensic planning include:

- Ability to gather digital evidence without interfering with business processes;
- Prioritising digital evidence gathering to those processes that may significantly impact the force, its staff and the communities it serves;
- Allow investigation to proceed at a cost in proportion to the incident or event;
- Minimise business disruptions to WMP; and
- Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action.

3.5 Line Managers

3.5.1 Managers are responsible for ensuring that their team and area of responsibility operates within the information governance framework of WMP. They will ensure that:

- There are effective methods for communicating information governance related issues within their team;
- Staff receive relevant training, induction and mandatory updates in relation to information governance;
- Staff are aware of information governance policies and encourage adherence to them;
- Necessary risk assessments are undertaken within their area of Responsibility; and
- Information governance issues and risks are discussed at any team meetings

3.6 ICT Security Manager

3.6.1 The majority of forensic investigations will use the ICT Security Manager as the technical investigative lead however in certain circumstances this role may be fulfilled by other WMP personnel such as the Forensics Team or delegated to a 3rd party.

In each case the technical investigative lead is responsible for –

- The management of forensic investigations;
- Maintaining a secure chain of evidence; and
- Ensuring appropriate external relationships are maintained, should an investigator independent of WMP be required. Note this may be delegated to a 3rd party but still managed by the investigative lead.

3.7 All Staff

3.7.1 All staff must maintain an up to date awareness of, and comply with, all WMP's policies and cooperate with the requirements of any investigating officer.

4. UNDERPINNING POLICIES AND PROCEDURES

4.1. To support the overarching Forensic Readiness 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;

5. EQUALITY IMPACT ASSESSMENT (EQIA).

5.1. 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.

6. HUMAN RIGHTS.

6.1. 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.

7. FREEDOM OF INFORMATION (FOI).

7.1. Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.3 of this policy has been GPMS marked as Not Protectively Marked.

7.2. 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		

8. TRAINING.

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

9. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

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

10. REVIEW.

10.1. 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.

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

10.3. 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.

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

10.5. 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

11. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	23 March 2015	Initial document	Tom King
0.2	24 March 2015	Some amendments to tie up with force policy.	Kate Jeffries
0.3	15 April 2015	Reformatted	Stephen Laishley
0.4	14 May 2015	Responses to feedback	Stephen Laishley
0.4	27/05/2015	Policy approved by CC, Have added signature and policy ref	56408 Couchman