WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Information Security Policy**
POLICY REFERENCE NO:	**Inf/06**

Executive Summary.

The purpose of this Information Security Policy (ISP - the Policy) document and supporting procedures is to set out the commitment of West Midlands Police (WMP) to protect West Midlands Police information, physical and personnel assets from all threats, whether internal, external, deliberate or accidental.

***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 all WMP Force personnel, i.e. Police Officers, Police Staff, Police Community Support Officers, Special Constables, volunteers, partners, agency or temporary staff, subcontractors and third-party suppliers who may use WMP information systems. Only current employees and vetted personnel as listed above will be granted access to WMP equipment, data and information systems. Access is granted to the information system on employment if a network account is required for the role.

Current Version And Effective Date.	**3.1**	**01/02/2019**
Business Area Owner	**Information Management**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries, Assistant Director Information Management**	
Policy Author	**Steve Yates, SIRA**	
Approved By	**CC Dave Thompson**	
Policy Initial Implementation Date	**17/10/2014**	
Review Date	**21/07/2021**	
Protective Marking	**OFFICIAL**	
Suitable For Publication – Freedom Of Information	**YES**	

Supporting Documents

- *APP* https://www.app.college.police.uk/app-content/information-management/information-assurance/
- *Code of Ethics (*http://www.college.police.uk/What-we-do/Ethics/Pages/Code-of-Ethics.aspx)
- *Acceptable Use Procedure*
- *Bluetooth Procedure*
- *Clear Desk Procedure*
- *Cryptographic Procedure*
- *Data Breach Procedure*
- *Government Security Classification Procedure.*
- *Information Security Incident Management Procedure*
- *Mobile/Remote Working Procedure*
- *Password Procedure*
- *Physical Security Procedure*
- *Protective Monitoring Procedure*
- *Retention/Disposal Procedure*
- *Subject Access Requests Procedure*

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 Vision

Preventing crime, protecting the public and helping those in need.

Force Diversity Vision Statement and Values

“Maximise the potential of people from all backgrounds through a culture of fairness and inclusion to deliver the best service for our communities”

“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/What-we-do/Ethics/Pages/Code-of-Ethics.aspx 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 organisation to do the right thing.

CONTENTS

ACRONYMS

- DCC – Deputy Chief Constable
- DPO – Data Protection Officer
- IAO – Information Asset Owner
- ISM – Information Security Manager
- ISMS – Information Security Management System
- ISAO – Information Security Assurance Officer
- SIMB – Strategic Information Management Board
- SIRO – Senior Information Risk Officer
- SIRA – Security and Information Risk Advisor
- SPF – Security Policy Framework
- SSO – Senior System Owner
- SyOPs – Security Operating Procedures

1. INTRODUCTION.

1.1. The purpose of this Information Security Policy (ISP - the Policy) document and supporting procedures is to set out the commitment of West Midlands Police (WMP) to protect West Midlands Police information, physical and personnel assets from all threats, whether internal, external, deliberate or accidental.

1.2. This Policy has been checked against APP. West Midlands Police has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by West Midlands Police. Those provisions are shown in the links below and can be accessed via the home page of the APP website:

https://www.app.college.police.uk/app-content/information-management/information-assurance/

2. INFORMATION SECURITY OBJECTIVES.

2.1. This Policy is a key component of WMP overall information security management framework and should be considered alongside more detailed information security documentation including relevant security guidance and procedures relating to Information Security and Assurance.

2.2. It is the Policy of WMP to ensure that:

- ✓ Information and physical assets will be protected against unauthorised access;
- ✓ Confidentiality of all assets will be assured;
- ✓ Integrity of information will be maintained;
- ✓ Regulatory and legislative requirements will be met;
- ✓ Information Security training will be provided;
- ✓ All breaches of Information Security, actual or suspected, will be reported and investigated;
- ✓ Business requirements for the availability of information and information systems will be met; and
- ✓ All Managers are directly responsible for implementing the Policy within their business area, and for the adherence by their staff.

2.3. The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WMP by:

- ✓ Identifying through appropriate risk assessment, the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk;
- ✓ Managing the risks to an acceptable level through the design, implementation and maintenance of a formal Information Security Management System (ISMS);
- ✓ Compliance with any third party or delivery partner contract/agreement conditions relating to information security;
- ✓ Commitment to comply with HMG's Security Policy Framework (SPF);
- ✓ Commitment to achieve and maintain accreditation under the National Police Chief's Council Information Systems Community Security Policy;
- ✓ Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies;
- ✓ Describing the principles of security and explaining how they shall be implemented in the Force;

- ✓ Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities;
- ✓ Creating and maintaining within the Force a level of awareness of the need for information security as an integral part of our day to day business; and
- ✓ Protecting information assets under the control of the Force.

2.4. It is the responsibility of each employee or third-party representative to adhere to this Policy. WMP recognise the importance of Force information assets and supports the goals and principles of effective security management to safeguard the confidentiality, integrity and availability of all information held. Therefore, it is important that there be in place sufficient and adequate information security safeguards and countermeasures to be able to provide the continued availability of Force information and information systems both internally and to policing partners.

3. ROLES AND RESPONSIBILITIES.

3.1. Information security is a responsibility shared by all members of the Force but ultimate responsibility rests with the Chief Constable.

3.2. Roles with specific responsibility for delivering information security are as follows:

- ✓ Senior Information Risk Owner (SIRO): The Deputy Chief Constable (DCC), as the SIRO, holds the responsibility of understanding how the strategic aims of West Midlands Police may be affected by failures in the secure use of the organisation's information systems;
- ✓ Senior System Owner (SSO): The Head of Information Technology as the SSO, is responsible for providing assurance to the SIRO that all Force information systems processing classified information comply with the requirements as laid down by Government, and other Regulatory bodies;
- ✓ Information Security Manager (ISM): The ISM is responsible for co-ordinating all aspects of security and providing advice required to necessitate the established information security standards necessary to safeguard information assets. The ISM is additionally responsible for the investigation of security incidents and providing security advice and guidance throughout the Force;
- ✓ Force Accreditor: All internal and external systems used to process classified material must be accredited. The Accreditor will act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting business requirements and to formally accredit systems on behalf of the Force;
- ✓ Information Security Assurance Officer (ISO)/Security and Information risk Advisor (SIRA): The ISAOs and SIRAs will provide security assurance expertise and ensure effective liaison and co-ordination of ICT security matters during the development, implementation and maintenance of information systems and technical equipment;
- ✓ Information Asset Owners (IAO): IAOs are senior people responsible for their business areas and the information that is processed/stored/accessed therein. Their role is to understand the information management process within their area of responsibility, what information is added and what is removed or destroyed, how information is moved/archived and who has access and why. Through this understanding, with advice from the Information Management and Security teams, they will provide assurance to the SIRO that the appropriate security measures are in place to protect their assets and that their staff have the appropriate information assurance training required for their roles;
- ✓ Data Protection Officer (DPO): The DPO is responsible for ensuring Force use of data is compliant with legislation, providing information and guidance on the

processing of all personal data and handling requests from data subjects in exercising their rights to access data and the rectification of any concerns;

- ✓ Employees and Non-Police Personnel Working for the Force: Following the provision of initial guidance and training, individual members of staff, including contracted staff and police volunteers, will be required to comply with the requirements of this policy and associated working practices, including specific system Security Operating Procedures (SyOPs) where these are in place. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard. Failure to do so may result in disciplinary action;
- ✓ Line Managers shall be individually responsible for the security of their physical environments where information is processed or stored. They are also responsible for ensuring that their permanent, temporary staff, and contractors are aware of the information security policies and procedures applicable in their work areas, their personal responsibilities for information security, and how to access advice on information security matters;
- ✓ The WMP Audit Team are responsible for the internal auditing of systems; reviewing, monitoring and documenting legal requirements as required and reporting to the SIRO any shortcomings discovered whilst carrying out these operations
- ✓ The Strategic Information Management Board (SIMB) under the direction of the SIRO, is responsible for the strategic management of Information Assurance and Security, the allocation of responsibilities, and the review / approval of change to the security architecture and documentation

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 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.

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 WMP (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. All official policy/procedural guidance documents will be considered for publication under the principles of FOI on the external website for public disclosure. Please see the ICO Definition Document for Police Forces for further details https://ico.org.uk/media/for-organisations/documents/1280/definition_document_for_police_forces.pdf

7. TRAINING.

7.1. Appropriate training shall take place for each group of responsible persons; this will include induction training on appointment or transfer and further specialist training as required and as appropriate.

7.2. Specialist training shall take place in particular for the roles of DPO, SIRA, ISM, Force Accreditor, IAO.

7.3. Induction training and update training/briefings shall take place for all other employees, such as Line Managers and general users of systems.

8. PROMOTION / DISTRIBUTION & MARKETING.

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

- Noticeboard message
- Publication onto the Policy Portal

9. REVIEW.

9.1 The policy business owner Information Security, 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.

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 by the date shown 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.
1.1	07/08/2014	Amended to new WMP format	Stephen Laishley/Paul Richards
1.2	12/08/2014	Policy/Procedure amendments	Stephen Laishley/Paul Richards
1.3	13/08/2014	Format amendment	Stephen Laishley/Paul Richards
2.0	18/08/2014	Final Version for Consultation	Stephen Laishley/Vicki Couchman
2.1	15/09/2014	Post Consultation Version	Stephen Laishley
2.2	09/10/2014	Amendment to policy/procedure details and clarification regarding the term staff and its application to police officers.	Stephen Laishley
3.1	01/02/2019	Policy reviewed and amended	Ashley Parker/Craig Moan/Steve Yates
3.1	21/07/2019	Policy approved by CC	56408 Parkinson

11. RELEVANT PROCEDURAL GUIDANCE.

(Please see policy portal page under Procedural Guidance and Supporting Documents)

Acceptable Use Procedure

Bluetooth Procedure

Clear Desk Procedure

Cryptographic Procedure

Data Breach Procedure

Government Security Classification Procedure.

Information Security Incident Management Procedure

Mobile/Remote Working Procedure

Password Procedure

Physical Security Procedure

Protective Monitoring Procedure

Subject Access Requests Procedure