WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Information Risk Management**
POLICY REFERENCE NO:	**Inf/34**

Executive Summary.

The purpose of this Information Risk Management Policy (IRMP - the Policy) document and supporting procedures is to set out the commitment of West Midlands Police (WMP) to protect WMP information, physical and personnel assets from all information risks. This policy outlines the governance requirements, the appropriate roles and responsibilities, and methodologies to be employed for ensuring the continued protection of National and Regional Information Systems and Assets. These will be achieved by the identification, review, escalation and treatment of risks, and how these risks will be proportionately and cost effectively managed.

***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.	**1.0**	**01/02/2019**
Business Area Owner	**Information Management**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries, Assistant Director, Information Management**	
Policy Author	**Steven Yates, SIRA, Information Management**	
Approved By	**CC David Thompson**	
Policy Initial Implementation Date	**21/07/2019**	
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)
- *RISK APPETITE STATEMENT.*
- *COMPLIANCE, AUDIT AND ASSURANCE PROCEDURE.*
- *INFORMATION ASSET OWNERS PROCEDURE (HANDBOOK).*
- *INFORMATION SHARING PROCEDURE.*
- *FORENSIC READINESS PROCEDURE.*
- *INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE .*
- *INFORMATION RISK MANAGEMENT PREVIOUS SUB POLICY INF/18*

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 POLICY PORTAL PAGES 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
- DPA2018 – Data Protection Act 2018
- DPO – Data Protection Officer
- GDPR – General Data Protection Regulation
- IAO – Information Asset Owner
- ICO – Information Commissioner's Office
- IS&A – Information Security & Assurance (Team)
- LED – Law Enforcement Directive
- SIRA – Security & Information Risk Adviser
- SIRO – Senior Information Risk Officer
- SPF – Security Policy Framework
- WMP – West Midlands Police

1. INTRODUCTION.

1.1. The purpose of this Information Risk Management Policy (IRMP - the Policy) document and supporting procedures is to set out the commitment of West Midlands Police (WMP) to protect WMP information, physical and personnel assets from all information risks. This policy outlines the governance requirements, the appropriate roles and responsibilities, and methodologies to be employed for ensuring the continued protection of National and Regional Information Systems and Assets. These will be achieved by the identification, review, escalation and treatment of risks, and how these risks will be proportionately and cost effectively managed.

1.2. This Procedure has been checked against APP. WMP has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by WMP. 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. REQUIREMENTS.

2.1. This policy stipulates the Information Risk Management (IRM) requirements necessary to enable appropriate levels of reassurance to be gained. This is due to:

- ✓ The increased reliance on National and Regional Information Systems and policing information by Forces, Agencies, Criminal Justice, local government partnerships and others;
- ✓ The ever-changing threat landscape to and introduction of new technologies in UK Policing;
- ✓ Collaborative working;
- ✓ Changes in data handling requirements and legislation;
- ✓ Increased personal, organisational liability and accountability; and
- ✓ The need to protect this information and the assets used to deliver it is greater than in previous years.

2.2. To address these issues it is necessary to ensure National and Regional Information Systems and assets in use by West Midlands Police are robustly, but proportionately and cost effectively, risk managed.

3. RISK APPETITE.

3.1. The Risk Appetite Statement is a separate document, reviewed and approved by the SIRO annually. It sets the background against which the force manages its Information risks**.** In line with best practice, WMP's risk appetite is set in the context of confidentiality, integrity and availability. There are five categories of risk appetite and the descriptions of the associated behaviours are as follows:

- ✓ **Averse (Risk Avoidance)**: Avoidance of risk and uncertainty is a key objective. Exceptional circumstances are required for any acceptance of risk;

- ✓ **Minimalist**: Preference for ultra-safe options that have a low degree of inherent risk and only have a potential for limited business benefit;

- ✓ **Cautious**: Preference for safe options that have a low degree of residual risk and may only have limited potential for business benefit;

- ✓ **Open**: Willing to consider all options and choose the one that is most likely to result in successful delivery minimizing residual risk as far as possible, while also providing an acceptable level of business benefit; and

- ✓ **Hungry (high risk, high reward):** Eager to realise business benefits and to choose options to achieve this despite greater residual risk.

4. INFORMATION ASSURANCE RISK MANAGEMENT.

4.1. There are three areas of Information Assurance (IA) risk management, defined as follows:

- ✓ **Confidentiality** – ensuring the information is accessible only to those authorised to have access;

- ✓ **Integrity** – safeguarding the accuracy and completeness of information and processing methods - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later; and

- ✓ **Availability** – ensuring that authorised users have access to information and associated IS when required.

4.2. Confidentiality, integrity and availability are all equally important. Although integrity and availability have always been key considerations, policy has tended to focus on confidentiality. This process ensures that all three are fully addressed and given equal importance. It recognises that many assets may have little or no requirement for confidentiality but availability and integrity may be vital and also that confidentiality extends beyond government protective markings to privacy and other sensitivities.

5. INFORMATION ASSURANCE KEY ROLES.

Data Controller.

5.1. The Chief Constable is the Data Controller for WMP.

Senior Information Risk Owner (SIRO).

5.2. By appointing a SIRO, WMP demonstrate that there is a mechanism and decision-making processes in place, at senior level, to consider appropriate technical and/or organisational measures for the type of information (including personal data), together with any risks to information and the business. The SIRO for WMP is the Deputy Chief Constable (DCC).

Data Protection Officer (DPO).

5.3. Within WMP, the Data Protection Officer (DPO) is an appointed police staff member within Information Management and is responsible for managing the Chief Constable's statutory obligations in respect of the DPA2018 (including GDPR and the LED). This includes notification to the Information Commissioner of the processing of personal information and any data processing breaches.

5.4. The DPO is responsible for the following:

- Advising the force and its Officers and Staff of its obligations under the DPA2018 (GDPR);
- Monitoring compliance with this Act and other relevant data protection law, WMP's policies with respect to this and monitoring training and audit activities relate to DP compliance;
- To provide advice where requested on data protection impact assessments;
- To cooperate with and act as the contact point for the Information Commissioner's Office (ICO); and
- Have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Information Asset Owner (IAO).

5.5. The Information Asset Owner (IAO) is responsible for all information in their business area. The DPO should assist the IAOs with their wider information management responsibilities, including the need to:

- Identify what information assets are held and ensure information assets are registered with Records Manager;
- Ensure that data is collected and used fairly and lawfully;
- Ensure that data is fit for purpose, accurate and up to date;
- Ensure that appropriate retention policies are established and implemented; and
- Ensure there is effective liaison between the IAO with the DPO so that the rights of data subjects and other data protection obligations are met.

Further details about the role and responsibilities of the IAOs within WMP can be found in the **Information Asset Owners Procedure.**

Information Asset Leads.

5.6. Whilst the IAOs take overall responsibility for the IA, they can choose to appoint an Information Asset Lead (alternatively called an Information Asset Assistant or IAA), in order to help them manage the asset; Asset Leads are usually frequent users with a good understanding of the system. The Asset Leads will ensure that policies and procedures are followed by key staff; they will be responsible for identifying any actual or potential security incidents, consulting their IAO on incident management and ensuring that the information asset register is accurate.

All Managers/Supervisors.

5.7. It is the responsibility of all WMP Officers and Staff who have a supervisory role to ensure that their staff operate within the terms of the DPA2018 (including GDPR and the LED), and any associated Force policies and procedural guidance. This must include regular checks of work to identify training and development needs in this area and to ensure that the quality of Force information assets is of a high standard.

All WMP Staff.

5.8. Every police officer, member of police staff, police community support officer, special constable, volunteer, data processor, contractor and approved persons working for or on behalf of WMP having access to personal data is required to comply with the requirements of the DPA2018 (including GDPR and the LED), and guidance contained

in operating rules, conventions, policies and procedures for each system or business area designed to help achieve compliance.

5.9. Police Officers and Police Staff members who process personal data about any other individual must comply with the requirements of this policy. Everyone must ensure that:

- All personal data is kept securely;
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data is kept in accordance with WMP's retention schedule;
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Compliance team;
- Any data protection breaches are swiftly brought to the attention of the Information Security & Assurance and that they support the team in resolving breaches;
- Where there is uncertainty around a data protection matter advice is sought from the Information Security & Assurance Team; and
- Ensure information provided to and held by WMP is accurate and up to date.

5.10. Where members of staff are responsible for supervising of others doing work, which involves the processing of personal information, they must ensure that those under their supervision are aware of the Data Protection principles.

5.11. Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Information Security & Assurance (IS&A) Team.

6. RISK ASSESSMENT.

6.1. Any individual or group of individuals that wish to commission a change to an existing system or implement a new one will initially discuss this with the appropriate IAO to gain approval in principle. If this change is commissioned through a formal project then this is the responsibility of the assigned project (or programme) manager.

6.2. The IAO will, either personally or through an approved delegate, discuss this change with the Security and Information Risk Advisor (SIRA). The SIRA will be responsible for gathering sufficient information to articulate a clear risk assessment of the proposal.

6.3. The risk assessment will be prepared based on the Security Policy Framework (SPF) which will generate a residual risk score after risk mitigation.

6.4. Risks will be treated in a reasonable and cost-effective manner and will not be overly mitigated in excess of what is needed to reasonably meet the risk appetite.

8. RISK ACCEPTANCE.

- ✓ *Once residual risk has been assessed it will move into the acceptance process.*
- ✓ *Risk can be accepted by different roles within the Force's information assurance structure.*
- ✓ *In the event that the risk cannot be accepted by the IAO, the SIRA will prepare a risk assessment and present it to the accreditor for discussion. Dependant on the risk matrix the Force Accreditor may be in a position to accept the risk.*

- ✓ *If the risk acceptance decision sits at SIRO level, then the Force Accreditor will produce an executive summary, showing risk, mitigation and residual risk for the proposal and present this to the SIRO.*
- ✓ *The SIRO will accept or reject the proposal and inform the Force Accreditor of the decision.*
- ✓ *It is the responsibility of the Force Accreditor to update the national body of any significant change.*
- ✓ *Usually the SIRO is the final decision maker for accepting local risks, however, in extreme cases it is possible to escalate a conflict to the Accounting Officer.*

9. EQUALITY IMPACT ASSESSMENT (EQIA).

9.1. 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.

9.2. *Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.*

10. HUMAN RIGHTS.

10.1. 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.

11. FREEDOM OF INFORMATION (FOI).

11.1. 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

12. TRAINING

12.1. Every network user must complete the National Centre for Applied Learning Technologies (NCALT) on-line training modules entitled 'Managing Information' within 3 days of joining the Force, and prior to gaining access to the corporate network. This training must be completed annually thereafter.

12.2. Successful completion of the following on-line NCALT training modules are a pre-requisite to obtaining access to Force information systems including obtaining an email account:

- Data Protection
- Managing Information;
- Freedom of Information;
- Government Security Classifications; and
- Fire Training.

12.3. All details of training commenced, progress, and completion are held centrally and accessible by the Force Data Protection Officer (DPO).

12.4. Non-completion may result in the individual being denied access to the Force network and all systems until the training is completed. In this event, the individuals Line Managers and Supervisors should assess the risk of leaving the individual in any role with unsupervised access to personal data and take action accordingly

12.5. All Line Managers and Supervisors should encourage individuals within their areas of responsibility to increase their data protection knowledge, and the obligations the DPA2018 Act places upon them, at every opportunity.

12.6. Individuals who leave and re-join the Force in a new role e.g. as a Special Constable, or who have had a break in service of more than 6 months, or are returning from long term sick, are required to repeat the training.

12.7. Information Asset Owners (IAOs) will receive bespoke training in addition to the above training packages.

13. PROMOTION / DISTRIBUTION & MARKETING.

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

- Publication onto force Policy Portal
- Noticeboard message

14. REVIEW.

14.1. 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.

14.2. 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.

14.3. 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.

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

14.5. 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

15. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
1.0	11/04/2019	Policy transferred back onto old corporate template	56408 Parkinson
1.0	21/07/2019	Policy approved by CC	56408 Parkinson

16. RELATED PROCEDURAL GUIDANCE

(See Policy Portal - Information Risk Management Policy page for copy)

RISK APPETITE STATEMENT.

COMPLIANCE, AUDIT AND ASSURANCE PROCEDURE.

INFORMATION ASSET OWNERS PROCEDURE (HANDBOOK).

INFORMATION SHARING PROCEDURE.

FORENSIC READINESS PROCEDURE.

INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE .