WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Joiners, Movers & Leavers**
POLICY REFERENCE NO:	**Inf/11**

Executive Summary.

The purpose of the Information Security policy is to protect WMP information assets from all threats, whether internal or external, deliberate or accidental. It is concerned with the preservation of:

- **Confidentiality -** ensuring that information is accessible only to those authorised to have access, disclosed only to those authorised to receive it, and so disclosed only for police purposes;
- **Integrity -** safeguarding the accuracy and completeness of information and information processing methods, and the ability to identify anomalies;
- **Availability -** ensuring that authorised users have access to information and associated assets when required.

All staff, including permanent, temporary, volunteers, contract staff, delivery partners and third party suppliers have a responsibility for safeguarding WMP's physical and data assets and ensuring the security of those assets at all times. The Information Security Force Policy document will help you to understand your responsibilities to fulfil them.

This Joiners, Movers & Leavers Policy underpins the Information Security Policy. It defines the key responsibilities and processes associated with resource changes within the Force – new starters, movers & leavers to the organisation. These responsibilities are key to safeguarding WMP's physical and data assets and ensuring the security of those assets at all times.

WMP's approach to information security is to balance the business requirements of the organisation with the potential harm and risk of an information security incident and the cost and logistics of implementing security controls.

If at any time the requirements of this document cannot be met these gaps MUST be raised with the Information Security Officer immediately.

***Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.*

Current Version And Effective Date.	**1.0**	**03/10/2014**
Business Area Owner	**Dean Sweet**	
Department Responsible	**Shared Services**	
Policy Contact	**Dean Sweet**	
Policy Author	**Dean Sweet**	
Approved By	**Chief Constable, Chris Sims**	
Policy Initial Implementation Date	**29/10/2014**	
Review Date	**29/10/2016**	
Protective Marking	**Not Protectively Marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*
- *Information Security Policy*
- *Recruitment Policy*
- *HMG Information Assurance Maturity Model (IAMM)*
- *HMG Security Policy Framework (SPF)*
- *Information Systems Community Service Policy (SCP)*
- *ACPO/ACPOS Police Service Information Assurance Strategy 2010 – 2013*
- *CESG IAS 1&2 Supplements – Information Risk Management Methodology*
- *ISO/IEC 27001:2005 Information Technology*

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.

Information is an asset that the organisation as a whole has a duty and responsibility to protect. The availability and accuracy of information is essential to West Midlands Police (which will now be referenced as WMP for the rest of this document) in functioning effectively and supporting of our policing objectives.

West Midlands Police holds and processes confidential personal information on private individuals, employees, partners and suppliers and also sensitive information relating to its own operational activities. In processing and storing this information the organisation has a responsibility to safeguard it and protect it from loss or misuse at all times.

The purpose of the Information Security Policy which this policy underpins is to set out a high level (Tier 1) framework of commitments by WMP, for the protection of the organisations information, supported by detailed Tier 2 Policies and Procedures aligned to HMG standards for Information Security. The objectives will be to:

Protect the organisation from threats to its physical, logical and information assets
Enable secure information sharing
Encourage consistent and professional use of data
Ensure everyone is clear about their role and responsibilities in using and protecting data
Ensure business continuity processes are established to minimise disruption;
Ensure compliance with HMG and ACPO/ACPOS policy
Ensure compliance with all relevant legislative and regulatory requirements and community obligations
Protect the organisation from legal liability and improper use of information.

In accordance with the HMG SPF Security Outcomes, this Information Security Policy (ISP) is the management directive for the implementation of controls supported by policy, standards, procedures and the relevant training and tools to protect WMP information assets.

The Joiners, Movers & Leavers Policy sets out the line manager responsibilities with regards to information security as set out in the BSI ISO Human Resource Security guidelines. The policy covers new starters (prior to employment) to the Force, movers (where roles of employees change) and leavers.

2. JOINERS.

Objective: To ensure that employees, contractors and third party users understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Core Responsibilities:

The recruiting manager will:

a. Ensure they understand the joiner process and what is expected of them

b. Ensure they understand the Forces Information Security Policy

c. Ensure they understand the Forces recruitment & screening processes

d. Ensure that prior to recruitment the security responsibilities are outlined to the candidates. This includes embedding them into the job description(s)

e. Build into the interview/selection process questions around awareness and application of information security

f. Identify at the outset what assets, access and general training the post holder(s) will require

g. Follow the Forces recruitment & screening process at all times

h. Highlight any concerns with Shared Services

i. Prepare a comprehensive Force induction programme covering; the role, the responsibilities assigned to the individual, the Forces Information Security Policy and associated policies, the assets associated with the role and the access permissions granted. The induction programme must identify relevant training for the individual and include the necessity of successfully completing the DP e-learning package as this is a pre-requisite for obtaining access to WMP systems and an email account.

Shared Services will:

a. govern and audit the joiner process including a 5% dip sample

b. advise & coach managers on how to apply the process

c. Process the screen element of the process and keep the recruiting manager updated

d. chase and escalate any non-compliance of the policy to the relevant Head of Department/ Commander

e. confirm back to the recruiting manager when all elements of the joiner process have been successfully completed

f. file all documentation relating to the new joiner electronically on the employee/ contractors e-personal file.

3. MOVERS/ CHANGE OF EMPLOYMENT

The process starts following the agreement of a change in role for a current employee/contractor or third party (this could be due to service redesign, change in business requirement, end of project, secondment, acting up, promotion or a complete change in role).

Core Responsibilities:

The existing & new line manager will:

a. Ensure they understand the movers process and what is expected of them

b. Ensure they understand the Forces Information Security Policy

c. Action all elements of the movers process in a timely manner

d. Document what assets and access rights the individual currently has and what the requirements of the new role are

e. Work together and develop & implement a joint action plan to ensure that the employee/ contractor/ third party does not have access rights or any assets that are not needed for the new role.

f. Ensure the employee/contractor/ third party understands their continued responsibilities under the Official Secrets Acts 1911-1989, the Data Protection Act 1998 and the Freedom of Information Act 2000.

g. Make arrangements for the employee/contractor/ third party to receive the appropriate assets and access levels associated with the role

h. Ensure that as part of the individuals induction to the new role that they are reminded of the Information Security Policy and how it applies to the role they are performing and identifying any relevant training

i. Report any non-compliance of this process to Shared Services.

The employee/ contractor/ third party will:

a. ensure they understand the process and what is expected of them

b. ensure they understand their continued responsibilities under the Official Secrets Acts 1911-1989, the Data Protection Act 1998 and the Freedom of Information Act 2000.

c. comply with all elements of the leaver process

d. return all of the organisational assets that they have in their possession that are no longer required in the new role to their line manager.

Shared Services will:

a. ensure this policy remains up-to-date and in line with business need

b. govern and audit the mover process including a 5% dip sample

c. advise & coach managers on how to apply the process

d. chase and escalate any non-compliance of the policy to the relevant Head of Department/ Commander

e. file all documentation relating to the termination electronically on the employee/ contractors e-personal file.

Departments who have issued assets/ granted access rights will:

a. ensure that following confirmation from the line manager that the role of an employee/ contractor/ third party is changing that line managers hand over assets that they have collected from the employee/ contractor and any access rights are removed

b. chase and escalate any non-compliance of the policy to the relevant Head of Department/ Commander.

Process Step		**Assigned To**
1.	Upon Shared Services receiving a notification/ being aware of a change in role for the employee/ contractor Shared Services will send a prompt to the existing & new line manager reminding them to complete this process.	Shared Services
2.	Prior to the start date of the change in role for the employee/ contractor or third party the line manager with responsibility for the “new” role that the employee/contractor/third party is moving to must document what assets and access rights the role requires.	New line manager
3.	A conversation must take place between the new line manager and the existing line manger to identify & agree a joint action plan that identifies changes to the current assets and access that the employee/ contractor/ third party has in readiness and in line with the requirements of the new role. The purpose of this is to ensure that the individual does not have assets or access rights that are not needed for the new role. To do this: The existing line manager must make an assessment must what assets & access the current employee/contractor/third party has. By comparing the two sets of requirements a set of actions should be agreed and documented between the existing line manager and the new line manager. The actions should outline: a. what assets the employee/ contractor/ third party	Current line manager & new line manager

	currently has that must be returned b. what additional ones are required c. What access needs to be revoked d. What new access is required e. What training around information security is required f. Which departments need to be updated with regards to the change in role Each of these actions should be assigned an owner and a date when they will be actioned by. It is the responsibility of the action owners to contact the relevant departments to make these changes. It is the responsibility of the employee to return any assets identified as no longer required/relevant to the existing line manager.	
4.	The existing line manager should meet with the employee/ contractor/ third party to confirm the actions that have been agreed and the associated owners and timescales and what is expected of them (in terms of returning assets etc) The employee/contractor/third party should be reminded of their continued responsibilities under the Official Secrets Acts 1911-1989, the Data Protection Act 1998 and the Freedom of Information Act 2000, following a change in their role.	Existing line manager
5.	Once the employee/contractor/ third party have started in their new role the new line manager must update Shared Services to confirm that all actions associated with the return of assets and change of access has been completed.	New line manager
6.	Shared Services will escalate to any line managers that do not confirm that all actions have been completed within 10 days of the start date of the change of role. Shared Services will undertake a 5% dip sample and will ask to see documentary evidence that this process has been completed.	Shared Services
7.	Shared Services will scan all of the completed associated paperwork and place on the e-personal file and update the mover status to “completed”.	Shared Services

4. LEAVERS.

Objective:

To ensure that employees, contractors and third party users exit the Force in an orderly manner in line with the Forces Information Security Policy and Information technology, Security techniques Code of practice for information security (BS ISO/IEC 27002:2005). The employee, contractor or third party users exit from the Force must be managed and all assets assigned to the individual returned and all access rights removed.

Core Responsibilities:

The line manager will:

a. Familiarise themselves and ensure they understand the Forces Information Security Policy

b. Ensure they understand the leaver process and what is expected of them

c. Explain the leaver process to the employee/contractor and clarify any questions they may have

d. Action all elements of the leaver process in a timely manner

e. Ensure the employee/contractor understands their post termination responsibilities under the Official Secrets Acts 1911-1989, the Data Protection Act 1998 and the Freedom of Information Act 2000.

f. Thoroughly & accurately complete the leaver form and return to Shared Services

g. Identify the organisational assets that the employee/contractor have in their possession and ensure that they return all of them

h. Ensure that the employee/contractor returns any assets they have

i. Return all of the assets collected from the employee/ contractor to the relevant Force departments

j. Return the completed termination checklist to Shared Services confirming that all stages of the process have been actioned

k. Report any non-compliance of this process to Shared Services

The employee/ contractor will:

a. ensure they understand the process and what is expected of them

b. ensure they understand their post termination responsibilities under the Official Secrets Act 1989, the Data Protection Act 1998 and the Freedom of Information Act 2000.

c. comply with all elements of the leaver process

d. return all of the organisational assets that they have in their possession to their line manager.

Shared Services will:

a. ensure this policy remains up-to-date and in line with business need

b. govern and audit the leaver process including a 5% dip sample

c. advise & coach managers on how to apply the process

d. process terminations in a timely manner and issue leavers letters to employees

e. alert all relevant departments (that have issued or given access to assets) regarding the employees/contractors termination date

f. chase and escalate any non-compliance of the policy to the relevant Head of Department/ Commander

g. confirm back to the line manager when all elements of the leaver process have been successfully completed

h. file all documentation relating to the termination electronically on the employee/ contractors e-personal file.

Departments who have issued assets/ granted access rights will:

a. ensure that following confirmation from Shared Services that an employee/ contractor is leaving that line managers hand over assets that they have collected from the employee/ contractor and any access rights are removed

b. chase and escalate any non-compliance of the policy to the relevant Head of Department/ Commander.

Termination (Leavers) Process

The process starts following the agreement of a termination date between the employee and line manager.

Process Step		Assigned To
1.	Line manager to meet with employee/ contractor to set out the leavers process, agree the termination date and complete stage 1 of the leaver process (the leavers form).	Line Manager
2.	In the meeting the line manager will: a. Explain the leavers process to the employee/contractor and their associated responsibilities b. Confirm the termination date c. Complete stage 1 of the termination process **"Leavers Form Part 1**" This form will capture: ▪ Employee Name/ Contractor Name ▪ Collar Number ▪ Post Number ▪ Job Title	Line manager

	▪ Grade ▪ LPU/ Department & Location ▪ Date of termination ▪ Reason for termination ▪ Home address (to check that we have the correct contact details held on systems within Shared Services) ▪ Any annual leave that has been overtaken or undertaken ▪ Confirmation that it has been explained to the employee/contractor that they must return all of the organisations assets to the line manager prior to leaving and the process for doing this (as outlined in the termination checklist) ▪ Confirmation that the employee/contractor has been reminded of their post-employment responsibilities under the Official Secrets Acts 1911-1989, the Data Protection Act 1998 and the Freedom of Information Act 2000.	
3.	Line managers must ensure that stage 1 of the leavers process (Leavers form part 1) is completed and sent to Shared Services immediately following this meeting. Any delays may result in overpayment of salary and continued access to the Force's systems following the termination date.	Line Manager
4.	Shared Services will process the leavers form within 3 days of receipt (or immediately if required due to late notification of leaver) and enter the termination date into Oracle. This will trigger the removal of access rights, this process is set out in the **Removal of Access Rights procedure.**	Shared Services
5.	Shared Services will notify PSD of the future leaving date. PSD will confirm whether or not the employee/contractor has any outstanding grievances or disciplinary investigations.	Shared Services & PSD
6.	Shared Services will issue a notification to all relevant departments that have issued assets or given access to information regarding the employees/contractors leave date. Following the notification it is the responsibility of the individual departments to ensure that line managers return the assets.	Shared Services
7.	Shared Services will issue a leavers letter directly to the employee confirming their leave date, reminding the employee/contractor of their responsibility to return all organisational assets assigned to them and of their post termination responsibilities under the Official Secrets Acts 1911-1989, the Data Protection Act 1998 and the Freedom of Information Act 2000.	Shared Services

8.	Prior to the employee/contractor leaving the line manager will complete the final element of the leavers process (stage 2) the leaver checklist. This checklist details all of the actions that must have been considered and completed prior to/on the employees/contractors final leave date. It is the responsibility of the employee/contractor to return all assets to the line manager. It is the responsibility of the line manager to ensure that the employee/contractor returns all assets and that these are then returned to the relevant departments. To support and govern this process Shared Services will contact the line manager 5 days before the leave date to ensure that this process is planned and underway. The completed checklist must be returned to Shared Services following the employees/contractors leave date. This will confirm that all of the associated actions with the Forces leaver process have been followed and completed.	Line Manager
9.	Shared Services will check this checklist and confirm back to the line manager once all of the leaver process has been successfully completed. Shared Services will escalate to any line managers that do not return the completed checklist within 5 days of the employee/contractor leaving.	Shared Services
10.	Shared Services will scan all of the completed leaver paperwork and place on the e-personal file and update the leaver status to completed.	Shared Services

5. EQUALITY IMPACT ASSESSMENT (EQIA).

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.

6. HUMAN RIGHTS.

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.

7. FREEDOM OF INFORMATION (FOI).

Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 1.0 (Draft) of this policy has been GPMS marked as **Not Protectively Marked.**

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.

Shared Services will deliver briefings to recruiting managers and line managers regarding this policy and the associated processes. They will also coach & guide managers through the process as they execute it. Shared Services will also monitor compliance to the procedures and increase/change training/coaching & mentoring in line with this.

9. PROMOTION / DISTRIBUTION & MARKETING.

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

- Intranet guidance
- Line manager and recruiting manager coaching & mentoring
- Advice & guidance via the telephone
- Line manager and recruiting manager briefings
- Attendance at LCT's

10. REVIEW.

The policy business owner Shared Services 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.

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.

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.

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

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.
0.8	12/09/2014	Draft	Dean Sweet, Shared Services Manager
0.9	13/09/2014	Draft for consultation	Dean Sweet, Shared Services Manager
1.0	03/10/2014	Amendments following consultation	Stephen Laishley & Dean Sweet
1.1	14/09/2014	Further amendments following consultation	Stephen Laishley & Dean Sweet