



WEST MIDLANDS POLICE

Force Policy Document

POLICY TITLE:	Information Sharing Agreements
POLICY REFERENCE NO:	Inf/05

Executive Summary.

To provide a framework for the management of information sharing agreements within the Force and to provide appropriate guidance to all staff.

This document replaces West Midlands Police Part One Order 04/2008.

***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 whether responsibilities include updating or simply using West Midlands Police information containing personal data.

Current Version And Effective Date.	V1.1	28/07/2014
Business Area Owner	Information Management	
Department Responsible	Intelligence	
Policy Contact	Data Protection Manager	
Policy Author	Kate Firkins (51264)	
Approved By	ACC Forsyth	
Policy Initial Implementation Date	04/11/2014	
Review Date	04/11/2016	
Protective Marking	Not protectively marked	
Suitable For Publication – Freedom Of Information	Yes	

Supporting Documents

- ICO Data Sharing Code of Practice;
- ICO Data Sharing Code of Practice checklist;
- ACPO Data Protection Manual of Guidance;
- ACPO National Police Database Board: Guidelines on ISAs;
- NPIA Guidance on the Management of Police Information (second edition)
- Authorised Professional Practice (www.app.college.police.uk/app-content/information-management/sharing/)
- Data Protection Policy
- Force Security Policy
- Force Policy on Information Disclosure
- Records Management Policy
- Information Management Strategy
- Force ISA Guidance
- Force ISA template

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. GUIDANCE5
3. COMPILING A WMP ISA7
4. DISCUSSION WITH PARTNERS.....7
5. COMPILING A DRAFT PURPOSE SPECIFIC ISA.7
6. AGREE DRAFT ISA WITH PARTNER(S).....8
7. SIGN OFF AND IMPLEMENTATION.8
8. PUBLICATION.....8
9. REVIEW.....9
10. PROCESS OF SHARING POLICE INFORMATION OUTSIDE AN ISA.120
11. EQUALITY IMPACT ASSESSMENT (EQIA).120
12. RESPONSIBILITIES FOR INFORMATION SHARING.....12
13. HUMAN RIGHTS.....12
14. FREEDOM OF INFORMATION (FOI).12
15. TRAINING.....13
16. PROMOTION / DISTRIBUTION & MARKETING.13
17. REVIEW.....13
18. VERSION HISTORY.14

1. INTRODUCTION.

- 1.1 The West Midlands Police is committed to working in partnership with other agencies involved in providing services to the public. It is recognised that the exchange of relevant information between such bodies is fundamental to achieving an effective quality service.
- 1.2 The Chief Constable, together with other key partners in West Midlands, will produce, where necessary, information sharing agreements (ISAs) which set out a framework for information sharing across the respective organisations.
- 1.3 ISAs will meet specific business needs and be in an agreed format.
- 1.4 The Force Data Protection Manager will provide assistance in negotiating and producing ISAs to designated managers within Force who are appointed to produce such agreements.
- 1.5 The operational benefits of an ISA are:
 - They ensure consistency in the way information is shared;
 - They allow the police to place conditions on the way information will be handled by the partner agency and vice versa;
 - They ensure that information can be shared lawfully;
 - They can help to build confidence in the role that the police play in protecting the public.

2. GUIDANCE

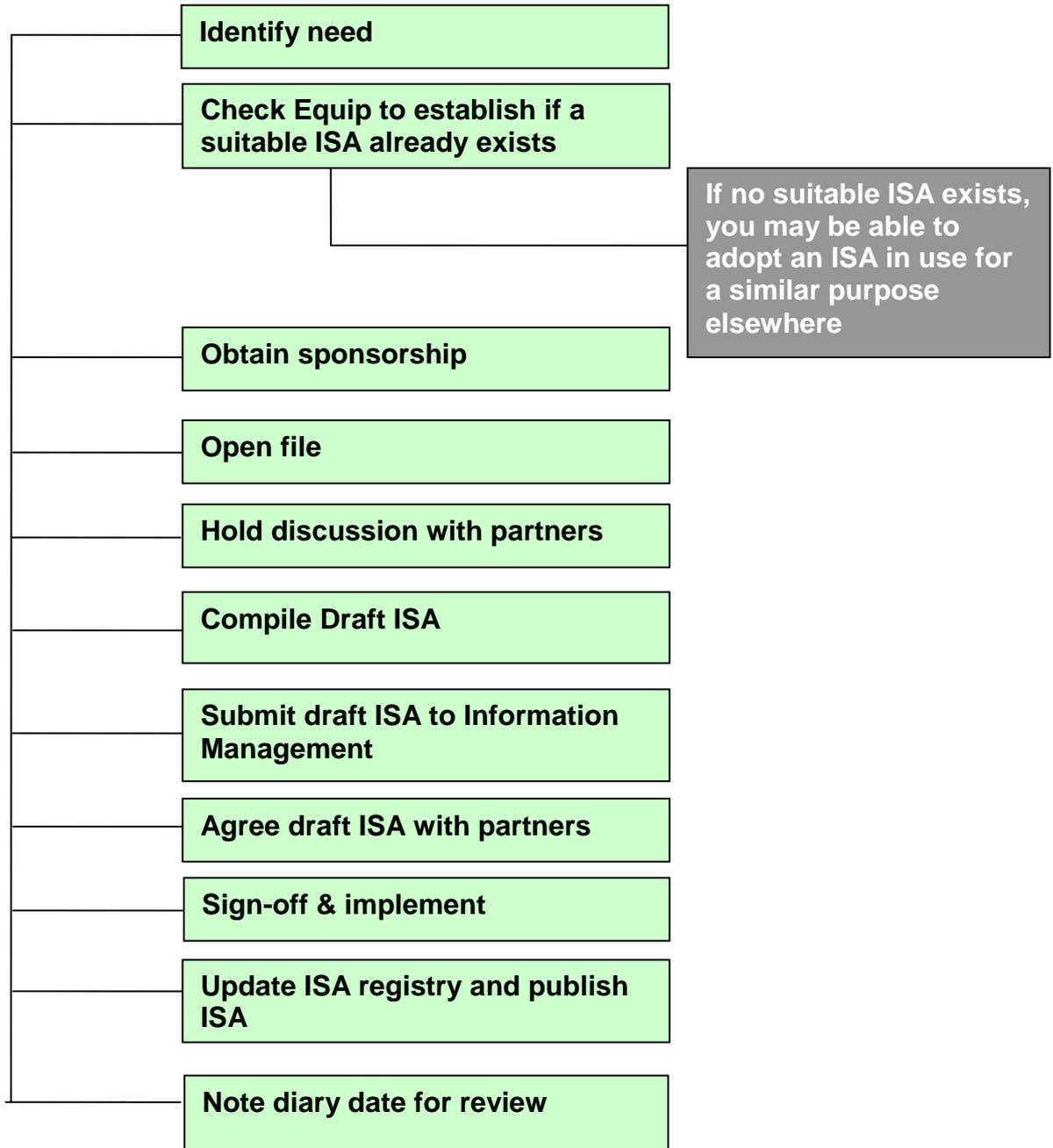
- 2.1 An Information Sharing Agreement would be required where a regular exchange of personal information is required between West Midlands Police and identified partners for a policing purpose.
- 2.2 Information can be shared without the existence of an ISA, for example, where the Chief Constable is directed under a Court Order; for the purpose of legal proceedings or where it is a simple ad hoc request.
- 2.3 Where it is identified by an LPU Commander or Head of Department that a business need exists for an ISA to be drawn up in order to facilitate the exchange of information between the Police and identified partner for a specific objective to be achieved, the following arrangements will apply:-
 - The relevant LPU Commander or Head of Department will appoint an ISA Sponsor (designated manager) to liaise with the partner organisations and oversee the development of any agreement on behalf of the Force.
 - The Force Data Protection Manager will provide assistance to the ISA Sponsor in negotiating and producing relevant agreements. The force template ISA is available [here](#).
 - Agreements will be drawn up and maintained locally by the ISA Sponsor responsible for the business area to which the ISA refers. The ISA will identify the types of information to be shared, under what circumstances, the Single Point of Contact (SPoC) for each party, and be signed off at an executive level by West Midlands Police and the identified partner(s) e.g. LPU Commander / Head of Department.
 - All proposed ISAs will be submitted to the Force Data Protection Manager for data protection compliance. The LPU Commander or Head of Department will endorse documents as appropriate on behalf of the Chief Constable.

NOT PROTECTIVELY MARKED

- The ISA Sponsor will retain overall responsibility for the management of their ISA and for reviewing and monitoring compliance with this policy.
- The identified Police SPoC will maintain a file, which will hold details of all Requests for Information, and Responses to Requests for Information, together with a copy of the ISA. During regular reviews by the Police SPoC, any information contained within the file that has been dealt with and no longer required, **will be retained for six years** from the date of provision of the information. This timescale meets minimum MoPI requirements, and also meets the timescale allowable for civil claims. The identified partner SPoC will also maintain a similar file.

2.4 Once authorised ISAs will be published for the benefit of the force on the intranet site, and on the Force Internet site, for the benefit of members of the public.

3. COMPILING A WEST MIDLANDS POLICE ISA



- 3.1 Before commencing the process of compiling an ISA, check Equip to see if a suitable agreement is already in place.
- 3.2 Once it has been identified that a business need exists for an ISA to be drawn up to facilitate the exchange of information between WMP and identified partners for a specific objective to be achieved, the relevant LPU Commander or Head of Department will appoint an ISA Sponsor.
- 3.3 The Sponsor should be a designated manager (Inspector or staff member equivalent) and be responsible for the business area for which the sharing is expected to provide benefits. They must be of sufficient seniority to sanction the development of the agreement and also be able to authorise the allocation of any necessary local resources that may be required.

NOT PROTECTIVELY MARKED

- 3.4 Specifically, the sponsor's responsibilities are:
- Validate and endorse the proposal (see below);
 - Agree that the benefits identified in the proposal are valid;
 - Agree to provide any appropriate resources to support both the development of the agreement and any activity that the proposed agreement is to support.
- 3.5 Sponsorship of an ISA is an enduring responsibility and does not end with the sign-off of the ISA. The sponsor's role includes promoting information sharing under the ISA and taking responsibility for ensuring the intended benefits of the ISA are realised.
- 3.6 The ISA Sponsor will be responsible for ensuring a 'file' or equivalent is created which should be used to record:
- The documented proposal and sponsor's approval from the previous step;
 - Any drafts of the stages used to create the ISA or the drafts of the completed ISA;
 - The original signed copy of the ISA (unless the original is held by a partner in which case a photocopy must be placed on the file);
 - The record of the annual review of the ISA (6 month review for new ISAs);
 - Any other material documents, faxes, hard copy e-mails or correspondence relevant to the ISA.

4. DISCUSSION WITH PARTNERS

- 4.1 If discussion has not already taken place with the identified partner, this should begin now. The purpose of the discussion is to:
- Put the identified partner(s) on notice that West Midlands Police will be seeking to enter into an ISA with them;
 - Obtain their initial views on the proposal, i.e.
 - The benefits of the information sharing;
 - The circumstances for sharing personal information;
 - What specific classes of personal information will be shared.
 - The legal power the identified partners will use if they are providing personal information to the force;
 - How the personal information will be transferred;
 - Understand if there are any special measures they will wish to see incorporated into the ISA;
 - Identify who the partner's contact point should be to progress development of the ISA.

5. COMPILING A DRAFT PURPOSE SPECIFIC ISA

- 5.1 At this stage a draft ISA can be created by:
- Using the Force ISA template;
 - Adapting an existing ISA;

6. AGREE DRAFT ISA WITH PARTNER(S)

- 6.1 Once the ISA sponsor is happy with the proposed ISA it will need to be registered with Information Management who will issue a unique ISA reference; record details of the ISA Sponsor; the ISA partners and the purpose of the proposed information sharing.
- 6.2 Information Management will maintain records of the version history and the Data Protection Manager will provide assistance to the ISA Sponsor.
- 6.3 The proposed ISA should be provided to the identified partners(s). Negotiations can then be conducted to arrive at a mutually agreeable process that is reflected in the text.
- 6.4 This may lead to some redrafting to accommodate the requirements put forward by identified partners. Changes will need to be cleared by the ISA sponsor.
- 6.5 This opportunity should be used to confirm the identified partners' contact details and the signatories that will feature in the final agreement.

7. SIGN OFF AND IMPLEMENTATION

- 7.1 Once West Midlands Police and identified partners(s) have agreed the contents of the ISA the following should take place:
 - The relevant LPU Commander or Head of Department and identified partners' representative(s) sign document;
 - Circulate copies to all identified partners;
 - Notify all members of staff likely to be affected and provide copies as necessary;
 - Send a signed electronic copy to Information Management for publication (see next step for details).
 - ISA Sponsor to retain original copy.

8. PUBLICATION

- 8.1 On receipt of an authorised Agreement which has been signed off by the relevant signatories, Information Management will arrange for it be uploaded to the Equip.
- 8.2 ISAs which have not been signed-off by the relevant signatory will not be uploaded to Equip and any information disclosed prior to an Agreement being signed-off may be deemed unlawful.
- 8.3 ISAs marked as 'Not Protectively Marked' will be published on the Freedom of Information (Fol) Publication Scheme, as per the Information Commissioner's Office (ICO) requirement.
- 8.4 ISAs with a 'Restricted' marking will not be published on the Fol Publication Scheme and not necessarily on the internal ISA Registry if in doing so it would prejudice the effectiveness of West Midlands Police or a partner organisation.

9. REVIEW

9.1 Where the ISA is in its first year, Information Management will provide a reminder after 6 months to the ISA sponsor for a review to be carried out in conjunction with the identified partner.

9.2 Thereafter, Information Management will provide a reminder to the ISA Sponsor for a review to be carried out on an annual basis.

9.3 The aim of the review is to ensure that the ISA is achieving its purpose and the actual sharing process is operating smoothly. The following will form part of the review:

Contacts: It is important to ensure that each identified partner still holds correct contact details for the key personnel operating or managing the data sharing;

Usefulness / Purpose: All identified partners should consider whether the information sharing is proving useful, and that the purposes for which it was established are still relevant to the work of the partners concerned. If the agreement is no longer useful it should be formally terminated

Basis: All identified partners should investigate whether any relevant legislation has been amended, or any new legislation enacted that would impact upon the agreement. If changes have taken place, the agreement may need to be amended to reflect this.

Incidents (Process): This is the opportunity for anyone involved to discuss any problems that have arisen regarding the process of exchanging the information (e.g. has the data been exchanged on time, have there been any complaints about its use etc).

Incidents (Security): This is the opportunity for anyone involved to discuss any security incidents that have occurred (e.g. unauthorised disclosures, physical/IT security failures). Credible assurances should be provided that any failures have been dealt with. Regular failures in security are likely to lead to the termination of the agreement.

Renewal / Termination: At the conclusion of the Review all identified partners parties should either renew the agreement for a further year, or terminate it.

9.4 Any security incidents must be investigated and discussed between identified partners the moment they come to notice.

9.5 The outcome of the review must be signed-off by the ISA sponsor and a copy placed on the registry file (see 2.5 above.).

9.6 If the review is not carried out within a timely manner, the Agreement will be withdrawn from circulation and any subsequent disclosure of information may be deemed unlawful.

10. THE PROCESS OF SHARING POLICE INFORMATION OUTSIDE OF AN ISA

10.1 Where an ISA does not exist, or the decision to share is a one-off, the following provides a reminder of the key questions that will help to ensure any information sharing is done lawfully.

- Who is asking for the information?
- Have you recorded their name, position, organisation and contact details?
- Have you verified the identity of the person requesting the information?
- What information is being asked for? What purpose will it be used for?
- Is the information being requested personal information?
- Has a legal gateway or a policing purpose to share information been established? If yes, how do they want the information?
- When do they want the information?
- Record your decision, how you made it and what information was shared.

11. RESPONSIBILITIES FOR INFORMATION SHARING

11.1 MANAGERS:

- Supporting staff to share information appropriately;
- Providing a system for recording decisions on whether or not to share information;
- Ensuring that all ISAs are held and managed centrally within force;
- Ensuring that the process of sharing information is adhered to by both those in a supervisory and user capacity;
- Authorising ISAs;
- Ensuring that staff who have a responsibility for sharing information are trained in accordance with the National Training and Delivery Strategy.

11.2 SUPERVISORS:

- Supporting staff to share information appropriately;
- Auditing, on an ad hoc basis, the decision to share made by users, including the necessity, accuracy and adequacy of information shared;
- Checking whether the decision to share meets a policing purpose or other legal duty or power;
- Ensuring that information being shared does not compromise any police operation or the safety of others;
- Ensuring that a risk-assessment process is adhered to by the user when making a decision to share information;
- Ensuring that ISAs are reviewed in accordance with force policy;
- Providing feedback to staff on their performance.

11.3 USERS:

- Ensuring that information is relevant, accurate and adequate for the purpose for which it is being shared;
- Ensuring that when personal information is shared, the requirements of the DPA and the common law duty of confidence have been fulfilled;

NOT PROTECTIVELY MARKED

- Applying a protective marking to the information being shared under the GPMS where applicable or a risk assessment where the sharing is carried out with the partners in the voluntary or private sectors who do not have a statutory purpose to share information;
- Recording any decision to share or not to share in accordance with the Information Management Strategy (IMS). Similarly, users are responsible for recording any decision not to share information on the relevant system;
- Ensuring that the information being shared meets a policing purpose or is lawfully disclosable for a statutory purpose and is proportionate and necessary;
- Following existing force policies set out in the IMS that comply with this guidance.

12. EQUALITY IMPACT ASSESSMENT (EQIA).

12.1 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.

13. HUMAN RIGHTS.

13.1 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.

14. FREEDOM OF INFORMATION (FOI).

14.1 Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 1.1 of this policy has been GPMS marked as not protectively marked

14.2 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

15. TRAINING.

- 15.1 All West Midlands Police officers and staff should familiarise themselves with this policy ensuring full knowledge.
- 15.2 Any identified specific training required to comply with this policy will be provided under the guidance of the Data Protection Manager.

16. PROMOTION / DISTRIBUTION & MARKETING.

- 16.1 The following methods will be adopted to ensure full knowledge of the Policy:
- 16.2 Policy document and associated documents on the force Intranet for the attention of all WMP Officers and Staff
- 16.3 Specific guidance available from the Data Protection Manager

17. REVIEW.

- 17.1 The policy business owner 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.
- 17.2 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.
- 17.3 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.
- 17.4 Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.
- 17.5 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

18. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
1.0	07/07/14	Review of policy 4/2008	51264 Firkins.
1.1	28/07/2014	Formatting amendments made	56408 Couchman