WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**WMP Online Research and Investigation Policy**
POLICY REFERENCE NO:	**INT/04**

Executive Summary.

This document outlines the criteria for carrying online research and investigation for WMP officers and Staff.

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

Intended Policy Audience.

This policy is aimed at all officers and staff of WMP who need to utilise the Internet to carry out any investigatory research.

Current Version And Effective Date.	**V2**	**14/09/2016**
Business Area Owner	**Intelligence**	
Department Responsible	**Force Intelligence**	
Policy Contact	**DCI Iain Donnelly**	
Policy Author	**DI Samantha Jones**	
Approved By	**ACC Foulkes**	
Policy Initial Implementation Date	**05/06/2014**	
Review Date	**14/09/2017**	
Protective Marking	**Official**	
Suitable For Publication – Freedom Of Information	**No**	

Supporting Documents

- *WMP Online Research and Investigation Policy*
- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*
-

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

"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/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 organisation to do the right thing.

CONTENTS

1. INTRODUCTION. 6
2. OPERATIONAL RISK CONSIDERATIONS. 7
3. LOCAL POLICY. 7
4. EVIDENTIAL CONSIDERATIONS. 7
5 CATEGORY GUIDANCE. 10
6. EQUALITY IMPACT ASSESSMENT (EQIA). 12
7. HUMAN RIGHTS. 12
8. FREEDOM OF INFORMATION (FOI). 12
9. TRAINING. 13
10. PROMOTION / DISTRIBUTION & MARKETING. 13
11. REVIEW. 13
12. VERSION HISTORY. 14
13. Appendix One 14
14. Appendix Two 17

Acronyms

ACPO	Association of Chief Police Officers
EQIA	Equality Impact Assessment
FOI	Freedom of Information
GPMS	Government Protection Marking Scheme
HRA	Human Rights Act
NPIA	National Policing Improvement Agency
SOP	Standard Operating Procedure
WMP	West Midlands Police
RIPA	Regulation of Investigatory Powers Act 2000
DRIPA	Data Retention and Investigatory Powers Act 2014
DPA	Data Protection Act 1998
CMA	Computer Misuse Act 1980
PACE	Police and Criminal Evidence Act 1984
CPIA	Criminal Procedure and Investigations Act 1996
MOPI	Management of Police Information 2010
NCALT	National Centre for Applied Learning Technologies
CAB	Covert Authorities Bureau
OSIR	Open Source Investigation Research
[redacted]	
NPCC	National Police Chiefs' Council
DSA	Directed Surveillance Authority
AO	Authorising Officer
OSC	Office of Surveillance Commissioners
SNS	Social Networking Sites
CHIS	Covert Human Intelligence Source
L&D	Learning and Development
NCA	National Crime Agency
WMCTU	West Midlands Counter Terrorism Unit
ASH	All Source Hub
CPD	Continuous Professional Development
OS	Open Source
LPU	Local Policing Unit
PPU	Public Protection Unit

1. INTRODUCTION.

Online communications via the internet has, in recent years, become the preferred method of communication with other individuals, within social groups or with anyone in the world with internet access. Such communication may involve web sites, social networks (e.g. Facebook), chat rooms, information networks (e.g. Twitter) and/or web based electronic mail.

'Open Source is defined as publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, newspapers, journals, TV and radio broadcasts, newswires, Internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute report).'

Examples of possible scenarios can be found at the end of this policy **(see Appendix One)**

This document provides the minimum standards that must be adopted by all persons engaged in open source investigation / research in order to maintain the integrity of any evidence gained and in order to avoid compromise of the following:

- The personal safety of individuals
- The hardware/software infrastructure of police computer systems
- Police tactics
- On-going and future police operations
- Reputational risks to WMP

Prior to any engagement in open source research staff should have a good understanding of any Legislation and Guidance that may apply and have carried out appropriate e-learning training packages:

- Human Rights Act 1998 (HRA)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Data Retention and Investigatory Powers Act 2014 (DRIPA)
- Data Protection Act 1998 (DPA)
- Computer Misuse Act 1980 (CMA)
- PACE 1984
- Criminal Procedure and Investigations Act 1996 (CPIA)
- Management of Police Information 2010 (MOPI)
- Police Act 1997
- Fair Investigations for Fair Trials – e-learning package
- ACPO 2012 Good Practice Guide for computer based electronic evidence
- NPCC Guidance on Open Source Investigation / Research

NCALT e-learning packages are available to assist in understanding of the issues involved.

- Management of Police Information – Level 1 – 4
- Communications Data in Investigations
- Introduction to Communications Data and Cybercrime
- Open Source Intelligence research- Initial Learning – Level 1
- NCALT Lawful Handling of Information

2. OPERATIONAL RISK CONSIDERATIONS.

[redacted]

Staff carrying out any type of open source investigation / research on the internet must be appropriately trained and are responsible for the security of information.

3. LOCAL POLICY.

5 Levels of Internet Investigation/Research

These 5 levels have been approved nationally to define the levels of activity for Open Source Investigation/Research (OSIR) **and** [redacted]

The first three levels are Open Source Investigation/Research and Covert Monitoring; [redacted]

NPCC Guidance on Open Source Investigation / Research is split into the following categories.

1. Open Source Intelligence/Research – covered by level 1 training [redacted]

(**Appendix One** provides an explanation of each level and what activity the user is likely to carry out).

4. EVIDENTIAL CONSIDERATIONS.

Processes must be in place to fully record and evidentially capture the contents of webpages that may contain material that is of evidential value. The (SOP) Standard Operating Procedure should be followed. (See Appendix Two)

This material should be available at a later date for audit and/or examination and any activity undertaken must be assessed to determine if a RIPA 2000 or Police Act 1997 authority is required.

[redacted]

[redacted]

Tasking of Open Source Research

Tasking of open source research should be made electronically using the appropriate tasking form. Complete the Request Details section, answering as many questions as possible, which should contain sufficient information and parameters to assist the researcher in conducting the research, except in extremely urgent cases, such as immediate threat to life, or dynamic situation e.g. kidnap and extortion investigation. In these circumstances the tasking form will be completed retrospectively.

When considering open source enquiries all staff are required to assess the necessity and proportionality in conducting the research, which may result in obtaining private information. The rationale for making the enquiry and decision making must be recorded within a Tasking Request Form.

Early consideration should be given to the requirement of an authority under RIPA 2000. In any event once the tasking is received, a further assessment will be made regarding such authority, by a supervisor within the Intelligence department.

If a Directed Surveillance Authority is deemed necessary, the responsibility for obtaining it will lie with the officer requesting the research, with the assistance of a trained RIPA applicant.

Sensitive Material

Should material be identified during the course of the research that may be considered sensitive, i.e. Legal Professional Privilege, Journalistic Material, Confidential Personal Information; the **activity should cease** and the information should be brought to the attention of an Intelligence Manager who **will** make the decision as to how this material is progressed and whether this needs to be brought to the attention of the AO (Authorising Officer) in the case of a DSA being in place.

Where the (OSIR) trained officer identifies material that is **not related** to the offences under investigation and is considered to be pornographic, obscene, abusive, inflammatory or otherwise suspicious, this should be recorded on the viewing record and brought to the attention of their line manager and OIC / SIO for consideration

Office of Surveillance Commissioners (OSC) Procedures & Guidance - Covert surveillance of Social Networking Sites (SNS)

288. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

288.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

288.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

288.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

288.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

5 CATEGORY GUIDANCE.

NPCC Level 1 - Overt Open Source Investigation/Research

- Basic research across publicly accessible search areas of the internet such as map viewing, news sites, local authority sites, auction sites or any publicly available website which has no requirement to register details to gain access.
- This activity would be considered as overt and would not require any RIPA or Police Act authority. Force policy regarding use of the WMP computer network must be adhered to.
- Staff conducting this activity must have completed the NCALT Open Source Intelligence Research – Initial Learning level 1.
- Overt interaction may only take place with individuals if the member of staff conducting the activity clearly identifies themselves as being a member of WMP staff, there is a clear policing purpose and an official WMP account is used e.g. Using WMP Twitter account to make direct contact with a missing person and urge them to make contact.

NPCC Level 2 - Core Open Source Investigation/Research

Only staff who have attended 3 day Open Source or 5 day Mainstream Cybercrime training can perform level 2 & 3 research[1]. [redacted]

- [redacted]
- Level 2 activities may require authority under RIPA 2000 or Police Act 1997 on a case by case basis with an assessment made by an intelligence supervisor / trained gatekeeper.
- Research to assist their investigations across the whole of the internet – using tools such as search engines; people search sites and social networks which may involve repeatedly visiting a particular site or page to show a pattern of behaviour.
- [redacted]
- [redacted]
- [redacted]

[1] College of Policing or those agreed by L&D
[2] Head of Confidential unit/Senior Intelligence Manager Force Intelligence

- Product recovered must be evaluated for intelligence purposes as well as evidential purposes and submitted into force/agency intelligence management systems using 3x5x2.

NPCC Level 3 - Covert Advanced Open Source Investigation/Research

- Level 3 activities will generally be undertaken by staff who have advanced skills and who work on dedicated Open Source Investigation Units. (E.g. All Source Hub (ASH) in London, NCA Open Source Unit, WMCTU Open Source Team etc.) [redacted]
- There is a higher likelihood that an authority would be required under RIPA 2000 or Police Act 1997 and the decision must be made by an intelligence supervisor / trained gatekeeper. Where there is ambiguity, guidance should be sought from Covert Authorities Bureau.
- Staff must have completed recognised advanced open source training to include relevant case law. If you are in any doubt as to the latest updates in case law please contact legal services.
- Product recovered must be evaluated for intelligence purposes as well as evidential purposes and submitted into force/agency intelligence management systems using 3x5x2.

The following NPCC Levels are not considered 'Open Source' tactics. However, in common with Levels 1 to 3, they are likely to involve the viewing and/or exploitation of well-known social networking and communication platforms.

NPCC Level 4 - [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Must be able to evidentially capture.
- Product recovered must be evaluated for intelligence purposes and submitted into force/agency intelligence management systems.

Supervisors should ensure that all searches are for an appropriate policing response. Failure to adhere to these principles may lead to the instigation of misconduct proceedings.

Level 5 - [redacted]

- [redacted]
- [redacted]
- [redacted]
- Product recovered must be evaluated for intelligence purposes and submitted into force/agency intelligence management systems.
- Training required. – [redacted]

"All Level 5 activity must adhere to WMP Policy, NPCC policy and OSC Guidance relating to CHIS activity"

6. 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.

7. 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.

8. FREEDOM OF INFORMATION (FOI).

Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 2 of this policy has been GPMS marked as Official.

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
	YES	

Reasons for Exemption – The policy discusses sensitive policing tactics that, if disclosed publicly, may impact on WMP ability to prevent and detect crime, target serious and organised crime and may jeopardise current and future investigations.

9. TRAINING.

The policy has been developed in conjunction with Learning and Development and the Covert Authorities Bureau. Staff attending future OSIR training will receive guidance in line with this policy and its appendices.

Staff should be provided with OSIR training in line with the requirements of their current role. Staff from departments outside of Intelligence, will be authorised to receive OSIR training where a business justification is made out and supported by their line manager.

10. PROMOTION / DISTRIBUTION & MARKETING.

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

This policy will be circulated and made available to all officers and staff of West Midlands Police in an operational, intelligence and investigatory capacity, via:

- Message of the day
- Force Intelligence website
- CPD Awareness days
- EQUIP Policy Portal

11. REVIEW.

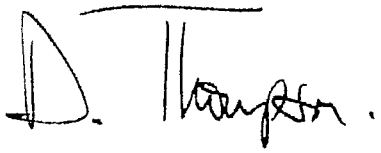
The policy business owner Force Intelligence maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

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

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
1.0	March 2014	First final draft completed	Ged Dowd
1.0	13/05/2014	Received and formatted	56408 Couchman
1.0	05/06/2014	Approved by CC and ACC – amended document for publishing	56408 Couchman
2.0	22/01/2016	Reviewed	DI Samantha Jones

13. Appendix One

Examples of Open Source Enquiries

General Research – Level 1

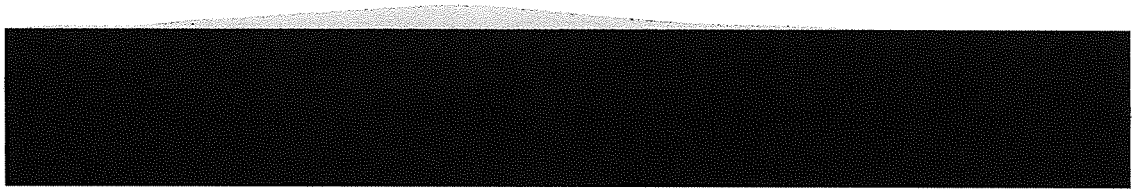
Scenario: An LPU has recorded an increase in the theft of catalytic converters from motor vehicles. It is suspected that they are being stolen for their scrap value. The Crime Manager has tasked (OSIR) trained officers to identify local scrap dealers who may be receiving the stolen catalytic converters.

Commentary: This is a basic search of information available to the public such as online business directories and search engines. This is a Level-1 enquiry which can be conducted on any computer.

EBay – Level 1

Scenario: An LPU has recorded an increase in burglary dwellings where the offenders are using specialist tools to 'pick locks' e.g. Bump keys. The Crime Manager has tasked (OSIR) trained officers to identify any people selling these tools on sites such as EBay & Gumtree.

Commentary: This is a basic search of information available to the public. The object of the search is the tool rather than specific individuals. This is a Level-1 enquiry which can be conducted on any computer.



EBay – Level 2

Scenario: A male has been arrested for handling stolen goods and his mobile phone was seized and analysed by E-forensics. The mobile telephone shows that the male is in control of an EBay account, from which he may sell stolen goods. (OSIR) trained officers have been tasked to review the EBay account and capture details of items he is selling.

Commentary: This is a single enquiry in relation to a specific individual which requires information to be captured for evidential purposes. This is Level-2 activity as the officer conducting the research should be competent in evidentially capturing data. A directed surveillance authority is unlikely to be required as the enquiry will be conducted on one occasion.

Online Grooming [Facebook] - Level 2

Scenario: PPU are investigating an allegation of online grooming involving a child being sent messages of a sexual nature by an adult on Facebook. (OSIR) trained officers have been tasked to capture the adults Facebook page and URL. The information will be necessary to prove the link between the suspect and the Facebook account used to contact the child and any data subsequently obtained from Facebook.

Commentary: This is a single enquiry in relation to a specific individual which requires information to be captured for evidential purposes. This is Level-2 open source research and the officer conducting the research should be competent in evidentially capturing data. A DSA is unlikely to be required to capture the profile page and URL. In order to capture private messages between the suspect and child, a one sided consensual Directed Surveillance Authority will be required. [redacted]

Initial Target Specific Intelligence Gathering – Level 3

Scenario: The Serious & Organised Crime Unit is investigating an individual involved in the supply of firearms. Dedicated (OSIR) staff have been tasked to fully document this individuals digital footprint across multiple social networking sites as part of the intelligence gathering stage of the operation.

Commentary: This is a single enquiry in relation to a specific individual to ascertain their presence on social media. This is Level-3 open source research, tasked to dedicated staff who will be confident in capturing data for evidential purposes. In the first instance a DSA may not be required, however further or repeated enquiries should be covered by a DSA. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

14. **Appendix Two**

Standard Operating Procedure (SOP) – Open Source Internet Research

Open Source Internet Research (OSIR) is widely understood to be a rapid growth area of business. There is a significant amount of open source activity which regularly features within WMP criminal investigations. This should be an effective and efficient procedure conducted in an auditable manner to ensure corporate consistency and compliance with ECHR, FOI, MOPI and DPA.

Internet Capture Files are the product of (OSIR). These files should be recorded in a viewable and retrievable format. A viewing log should be created by the person

capturing the information from the internet which will provide the lead investigator with detailed descriptions and summaries of the material contained within them.

Some of the captured information may be required as evidence. Any remaining information will become unused material. In order to comply with CPIA (Disclosure), a clear audit trail and assessment process is essential.

Terms of reference should be devised between the OIC / SIO and the (OSIR) trained officer and a strategy for the reviewing and storing of material should be agreed from the outset. This strategy will provide direction and guidance in relation to what material is sought and what may be relied upon as part of the investigation. This process should be reviewed regularly to ensure the terms of reference are being adhered to and expectations are being met.

Sensitive Material

Should material be identified during the course of the research that may be considered sensitive, i.e. Legal Professional Privilege, Journalistic Material, Confidential Personal Information; the activity should cease and the information should be brought to the attention of an Intelligence Manager who will make the decision as to how this material is progressed and whether this needs to be brought to the attention of the AO (Authorising Officer) in the case of a DSA being in place.

Where the (OSIR) trained officer identifies material that is not related to the offences under investigation and is considered to be pornographic, obscene, abusive, inflammatory or otherwise suspicious, this should be recorded on the viewing record and brought to the attention of their line manager and OIC / SIO for consideration.

SIO / OIC

1. The OIC and SIO/DSIO will agree terms of reference for the open source research strategy.

2. The strategy must be reviewed regularly to ensure terms of reference is being adhered to and expectations are being met.

3. The frequency of (OSIR) will be set according to available intelligence and in line with the SIO's operational objectives.

4. It will be the responsibility of the OIC and SIO/DSIO to ensure the appropriate authorities are in place to support the activity.

Open Source (OSIR) trained officer

1. The (OSIR) trained officer will conduct research in line with the terms of reference set out by the OIC and SIO / DSIO.

2. All activity conducted by the (OSIR) trained officer will be exhibited and recorded in a viewable and retrievable format.

3. A master disc and working copy will be provided to the OIC together with a statement.

A copy of the activity log will be retained by the intelligence department who will maintain a central record of all (OSIR) for research purposes and inspection.

15. Appendix Three

[redacted]