Ministry
of Defence Police

**MDP Secretariat**
**Room 126, Building 1070**
**MDP HQ Wethersfield**
**Braintree, Essex CM7 4AZ**

**Tel: 01371 85**[redacted]
**Fax: 01371 854080**
**E-mail: MDP-FOI-DP@mod.uk**

[redacted]

By email – [redacted]

Our Ref: eCase: FOI2016/09012 RFI: 267/16
Date: 22 December 2016

Dear [redacted]

**FREEDOM OF INFORMATION ACT 2000: MINISTRY OF DEFENCE POLICE: SOCIAL MEDIA MONITORING.**

I refer to your email dated 26th September 2016.

We are treating your email as a request for information in accordance with the Freedom of Information Act 2000 (FOIA 2000).

In your email of the 26th September 2016 you requested the following information:

**“1. For the time period 1.1.2015 to 1.10.2016**

**Please provide all information relating to guidance / policy / training on the obtaining, use, analysis, retention and destruction of:**

**a. SOCMINT: Social media intelligence**

**And/or**

**b. Online research and investigation and digital investigations and intelligence capability**

**And/or**

**c. OSINT: Open Source Intelligence**

**Please provide all information including: all related policies, training documents, codes of practice. Please include all information related to acquisition, use, retention, storage and destruction. If you use different terminology to refer to social media information and / or open source intelligence please note that our request is directed at that.**

**2. For the time period 1.1.2015 to 1.10.2016**

**Please provide all information relating to statutory guidance / guidance / policy / training on the use of fake profiles by the police on social media, including but not limited to Twitter and Facebook. Please include all information related to acquisition, use, retention, storage and destruction of information via this technique.**

**3. For the time period 1.1.2015 to 1.10.2016**

**Please provide all information relating to statutory guidance / guidance / policy / training on the use of SOCMINT and OSINT used for the purpose of profile building by the police including but not limited to Twitter and Facebook. Please include all information related to acquisition, use, retention, storage and destruction.**

**4. For the time period 1.1.2015 to 1.10.2016**

**Please provide all information relating to statutory guidance / guidance / policy / training on the recording, storing and use of OSINT (Open Source Intelligence). Please include all information related to acquisition, use, retention, storage and destruction.**

**5. Please provide information on whether you have a head of digital / lead on digital or the equivalent appointed."**

A search for the information has now been completed within the Ministry of Defence Police and I can confirm that some information in scope of your request is held.

You will recall when we wrote on 24th October 2016, we advised you that we would be completing a public interest test to determine whether all, or some, of the information should be released.

I have completed a public interest test and concluded that the release of the redacted material within the attached document would be prejudicial to MOD and MDP and that the public interest favours not releasing some of this information. I am therefore withholding some of the information in accordance with FOI exemption Section 31(1)(a) Law enforcement and Section 40(2)(3) Personal data.

> Section 31(1) Law enforcement applies because providing details of would reveal some information that would undermine the prevention or detection of crime and the administration of justice and would undermine the effectiveness of the department.
>
> Section 40(2)(3) has been applied to the names and contact details of staff in order to protect personal information as governed by the Data Protection Act 1998. Section 40 is an absolute exemption and there is therefore no requirement to consider the public interest in making a decision to withhold the information.
>
> Personal data is defined under Section 1(1)(e) of the DPA98 as "data which relates to a living individual who can be identified – (a) from those data".

**Questions 1-5.**

Please see attached document at Annex A. The MDP Internet Open Source & Social Networking Sites Research and Investigation was published January 2016. Prior to this date the Ministry of Defence Police applied the NPCC national guidance on OSInt data.

Any data including OSInt is managed, processed and retained/destroyed in line with the National MOPI framework and guidelines.

All Ministry of Defence Police Intelligence staff do the NCALT Level 1training course and the College of Policing Research, Investigate, Trace, Electronic Suspect (RIITES) training course for OSInt work.

There is no over-arching head or lead on digital within the Ministry of Defence Police.

If you are not satisfied with this response or wish to complain about any aspect of the handling of your request, then you should contact me in the first instance. If informal resolution is not possible and you are still dissatisfied then you may apply for an independent internal review by contacting the Information Rights Compliance team, 1st Floor, MOD Main Building, Whitehall, London SW1A 2HB (email CIO-FOI-IR@mod.uk). Please note that any request for an internal review must be made within 40 working days of the date on which the attempt to reach informal resolution has come to an end.

If you remain dissatisfied following an internal review, you may take your complaint to the Information Commissioner under the provisions of Section 50 of the Freedom of Information Act. Please note that the Information Commissioner will not investigate the case until the MOD internal review process has been completed. Further details of the role and powers of the Information Commissioner can be found on the Commissioner’s website (http://www.ico.org.uk).

Yours sincerely

**MDP Sec Data Protection and Freedom of Information Office**

# MDP Internet Open Source & Social Networking Sites Research and Investigation

# POLICY

Operational Capability Centre
Doctrine & Compliance

Effective from: (January 2016)

Created by: [redacted] (MDP Internet Open Source and Social Networking Sites Research and Investigation) (v1.0)

## TABLE OF CONTENTS

## 1. POLICY AIM

The aim of this policy is to maintain safety, integrity and compliance by regulating the Ministry of Defence Police (MDP) research and investigation of Internet Open Source and Social Media Sites.

The associated SOP will advise on and direct MDP officers and staff in the use of the Internet (open source, social networking and other internet sites) in conducting investigations and/or intelligence research/development.

## 2. APPLICABILITY

This is a new policy for MDP. There are no summary of changes. This policy should be read and applied by all MDP officers and staff when conducting research or investigation of Internet open source and Social media sites.

## 3. POLICY DETAIL

Rapidly increasing use of Internet open source and Social media sites across communities and businesses has resulted in law enforcement having access to an array of investigative tools. Internet open source and Social media sites contain a wealth of information, intelligence and evidence about suspects, victims, witnesses, protest activists, members of organised crime groups and other aspects of criminal and anti-social activity. Information contained in such sites has the potential to impact upon many aspects of policing.

It is vital that officers and staff of MDP who make use of information contained in Internet open source and Social media sites do so in a manner in accordance with the law, utilising an approach that achieves best evidence, protecting where necessary potentially sensitive police tactics.

## 4. IMPLICATIONS OF THE POLICY

### 4.1 Training Requirements

MDP Officers and staff carrying out any type of Internet open source and Social media sites research and or investigation must be appropriately trained relevant to the level of use/intrusiveness they are conducting. National Standard under development.

### 4.2 IT Infrastructure

Level 1: Internet open source and Social media sites research and investigations should be carried out on MDP computer equipment and devices that are fully attributable (overt) to the Police Service – MoD EGS accounts.

Level 2 – 5: Internet open source and Social media sites research and investigations should be carried out on MDP owned computer equipment and devices that are non-attributable (covert) to the Police Service.

[redacted]

[redacted]

MoD/MDP ITSyOps apply to all attributable and non-attributable computer equipment, devices and accounts.

### 4.3 Related Policies or Documents

Prior to engaging in any open source investigation/research MDP officers and staff should have a good understanding of the legislation and guidance that may apply:

- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Data Protection Act 1998
- Criminal Procedure and Investigations Act 1996 (CPIA) or Criminal Justice & Licensing (Scotland) Act 2010
- Management of Police Information 2010 (MoPI)
- OSC Procedures and Guidance Document 2014
- The Interception of Communications Code of Practice
- NPCC principles for recovery of digital/computer data
- Guidelines On The Safe Use Of The Internet And Social Media By MDP Officers
- MoD JSP740 Acceptable Use Policy
- MoD ITSyOps
- MDP Internet Open Source & Social Networking Sites Research and Investigation SOP

## 5. MONITORING AND REVIEW

At this time the Operational Capability Centre (OCC) Doctrine and Compliance team will be responsible for monitoring and reviewing this policy and will conduct a formal review of the efficiency and effectiveness of its application. This includes a review of the following measures:

- Feedback on the content of this policy from policy users.

- Environmental scanning of policy related matters (intranet and internet)
- Implementation of actions arising from Equality Impact Assessments

## 6. WHO TO CONTACT ABOUT THIS POLICY

ACC Organisational Development and Crime owns this policy with management of its content being devolved to the OCC doctrine policy team and author responsible for its specific content.