METROPOLITAN POLICE TOTAL POLICING

Freedom of Information Request Reference No:

I note you seek access to the following information:

1. Disclose any updated/additional guidance and policy on the use of open source intelligence and/or social media monitoring/intelligence.
I note previous disclosure attached.

2. Disclose any current contracts with providers of software and/or hardware and/or other services related to the conduct of social media monitoring.

DECISION

I have today decided to disclose some of the requested information. Some data has been withheld as it is exempt from disclosure and therefore this response serves as a Refusal Notice under Section 17 of the Freedom of Information Act 2000 (the Act).

The answer to **Question One** has been disclosed.

Information in respect of **Question Two** is held but has been exempt from disclosure by virtue of Section 31(1)(a)(b) (Law Enforcement).
(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—
(a)the prevention or detection of crime,
(b)the apprehension or prosecution of offenders,

In considering whether or not this information should be disclosed, I have considered the potential harm that could be caused by disclosure.

Disclosure of held information including the methods used would prejudice current and future investigations. Such information could, and would be used by those seeking to frustrate police investigations and would make the public less safe.

Additionally in respect of Question Two the MPS also neither confirm nor denies whether any other information is held by the MPS for your request by virtue of Section 23(5) (Information that may relate to security bodies) and 24(2) (National Security). Please note this exemption should not be taken to as an indication of whether or not any further information is held for this part of your request.

Section 23(5) of the Act provides:

(5) The duty to confirm or deny does not arise if, or to the extent that, compliance

with section 1(1)(a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3).

Section 24(2) – (National Security) of the Act provides:

(2) The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

It is in the public interest to neither confirm nor deny whether any further information is held in order to protect the security and infrastructure of the UK which would be compromised by an adverse FOIA disclosure.

Confirming or denying whether further information is held may frustrate policing tactics/methods and render security measures less effective, increasing the risk of harm to the public. This would not be in the public interest.

REASONS FOR DECISION

The MPS uses a range of internet collection and analysis tools/services to help keep London safe from many aspects of criminal behaviour and attack. Such methods greatly assist with the prevention and detection of crime and assist with the apprehension or prosecution of offenders, particularly in respect of the safeguarding of our national security.

DISCLOSURE

In respect of **Question One**, please find attached to this response letter the updated MPS document you have sought under FOIA.

I would like to take this opportunity to thank you for your interest in the Metropolitan Police Service.

Information Rights Unit

Title & Version	Internet & Social Media Use in the MPS: Guidance document Version 1.6
Author	Met HQ Information Assurance Unit (IAU)
Organisation	Met HQ Performance and Assurance
Summary	This guidance provides instructions and advice on how to access and use the Internet and social media securely and lawfully from MPS information and communications technology (ICT) systems

Internet & Social Media Use in the MPS: Guidance

APPLICATION

When? - This guidance document is operative with immediate effect.

Who? - **The Internet & Social Media Use guidance document** applies to all MPS Personnel and authorised users who are allowed to access/ use the Internet and social media from MPS ICT equipment via AWARE or other MPS ICT systems [including standalone computers and mobile devices], whether allowed for business or personal reasons.

Such users are required to comply with, all relevant MPS policy and associated procedures, specifically the Use of MPS Information & ICT Systems Policy Toolkit [published on corporate Policy Pages on 15 July 2013] which this guidance document supplements.

The Guidance document may refer to particular responsibilities or involvement for personnel in the following roles:

- (B)OCU Commanders/ Heads of Branches
- (B)OCU Line Managers or supervisors
- (B)OCU personnel undertaking Internet/ Social media research, intelligence or investigation
- (B)OCU Social Media Team Leaders (SMTL)/ Social Media Team personnel
- Digital Policing - Secure Services [Gateway Team]
- Digital Policing - Digital Services
- Met HQ Information Assurance Unit (IAU)
- MPS Data Protection Officer [Met HQ]
- Directorate of Media and Communications (DMC)
- SC&O39 Covert Governance & Intelligence Compliance - Inspection & Review Team
- SC&O Met Intelligence Bureau (MIB) - Open Source Team
- Directorate of Professional Standards (DPS)

OBJECTIVES

This Guidance document is one of a series produced by the IAU that document procedures or provide advice to ensure compliance with the Information Management Policy. Collectively this Guidance document seeks to:

- Protect the interests and investment of the MPS
- Maintain public confidence in police use of sensitive information
- Conform to legislative requirements
- Ensure operational police work is not jeopardised

These objectives are set to safeguard the organisation and its effectiveness. The objectives are achieved by making sure all MPS personnel and all other persons with authorised access to the Internet and social media understand and act upon guidance within this and other documents. It should be noted that this guidance is not intended to restrict the reasonable exercise of any individual rights and freedoms [such as private/ family rights or freedom of expression] in a democratic society.

This Guidance document is to be read, acted upon and interpreted in conjunction with the following documentation - All MPS personnel and authorised persons must familiarise themselves with such documentation prior to accessing or using the Internet and/ or social media:

- The MPS Information Code of Conduct v4.1 dated June 2013 [also found on the AWARE desktop];
- Use of MPS Information & ICT Systems Policy Toolkit [published on corporate Policy Pages on 15 July 2013];
- The AWARE Security Operating Procedures (SyOps) [accessible from the AWARE Foundation desktop]; and
- Any published guidance relating to a particular social media site [such as Twitter] - see DMC Digital and Social Media Team and Toolkit
- Internet investigation guidance - Met Operations and Intelligence Services - Online and Open Source Guidance and MIB Open Source Guidance
- ACPO Guidelines on Safe use of the Internet & Social Media January 2013

STATEMENT

The Metropolitan Police Service recognises that the Internet carries the largest amount of knowledge, information and services in history. Internet use has become incorporated and essential to many aspects of modern life including the work of the MPS. As a consequence there are benefits to policing in ensuring that MPS personnel are able to access the Internet to assist in their day to day work.

Various types of social media also provide opportunities for wider real time communication with individuals and communities in London and elsewhere in the interests of Total Policing. As a consequence it has been agreed on the authority of Management Board that:

- Access to the Internet and social media is extended in principle to all MPS personnel and other authorised persons
- Access and use is allowed primarily to assist MPS personnel in their duties whilst working [i.e. known as **business use**]
- In addition **personal use** of the Internet and social media is now permitted during working hours up to the point where it adversely impacts on an individual's ability to deliver their directed tasks or otherwise interferes with the individual's employment responsibilities or productivity. For further requirements go to Use of MPS Information & ICT Systems Toolkit - see Personal & Acceptable Use of MPS Information & ICT Systems - Frequently Asked Questions (FAQs)

You must do nothing which risks bringing the MPS into disrepute or compromises its effectiveness or the security of its operations or assets. To do otherwise might lead to disciplinary and/ or legal action, with potentially serious consequences for yourself and the organisation.

Data Protection Act Compliance

All staff need to be aware that processing of personal data must be conducted in compliance with the **Data Protection Act 1998 (DPA)** and this applies in all respects when using the Internet and social media. If personal information is taken from open source Internet pages, for say general research purposes, or is requested during social media interaction to better engage with the public, MPS staff must provide a link to the MPS Fair Processing Notice to all individuals whose personal data has been collected.

Managers' Supervisory Responsibilities

Line managers **must** actively supervise their staff with respect to the use of MPS Information and ICT.

In respect of the general supervisory function of managers/ supervisors and regarding dealing with suspected misuse of MPS ICT Systems, see instructions in the Use of MPS Information & ICT Systems Policy Toolkit - see Use of MPS ICT Systems - Manager/ Supervisor's Checklist

Personal security & identity guidance

Cyber criminals are increasingly using sophisticated methods of social engineering to target individuals and through them organisations such as the MPS. This can conceivably put you, your friends/ family, colleagues, the MPS ICT infrastructure and others at risk if due care and diligence is not exercised when accessing the Internet and social media. Following this

guidance document should assist in assuring the personal safety and personal identity of individuals and protect the reputation and integrity of the MPS.

It is therefore expected that MPS personnel and other authorised persons will conduct themselves so as to avoid bringing the MPS into disrepute; or otherwise compromising MPS effectiveness or the security of its operations/ assets whilst using the Internet and social media. Individuals are accountable for their own actions so you will need to exercise your own discretion and strike the right balance on what should be disclosed in various circumstances.

All MPS personnel and other authorised persons should therefore take account of the following when using the Internet and social media at work [either in a business or personal capacity]. For reasons of personal safety, to protect your identity and MPS ICT systems and information:

- You should avoid disclosing personal or sensitive details to an un-trusted third party
- To avoid compromising MPS security avoid undue references to police uniform, equipment, buildings or policing methods
- **Never** reveal the security clearances [vetting levels] of either yourself or that of another member of the police service to an un-trusted third party or by publishing such details
- Do not use MPS email addresses to authenticate with private sites or replicate the passwords you use on MPS system accounts when accessing private sites
- Ensure that you use the privacy and security settings available on social networking sites
- If you do disclose that you work for the MPS, then you **must** make it absolutely clear that any views expressed are yours alone and do not represent the official position of the MPS
- Remember that HMG and police service advice is that all public servants [including police personnel] should regularly review the content of both their work and personal on-line profiles. Regarding personal on-line profiles, see the valuable advice at **Section 8 - Keeping your private life private** [page 7] of the ACPO Guidelines on Safe use of the Internet & Social Media January 2013

PURPOSE AND SCOPE

This guidance document in conjunction with the Use of MPS Information & ICT Systems Policy Toolkit provides guidance on how to use the Internet and social media safely and lawfully. They set minimum standards and provide basic rules concerning what you are allowed to do and what is prohibited when using the Internet and social media at work [whether it is for police business or personal use]. General advice and guidance is also given where appropriate to assist users of the Internet and social media, particularly where they can apply their discretion. In this way MPS personnel and authorised persons should better understand what is regarded as acceptable; or conversely what constitutes improper use of the Internet or social media.

It is expected that line managers will enforce this guidance document through positive tasking and active supervision.

Access to the Internet or social media services can be through the MPS ICT infrastructure; from designated MPS standalone computers or from approved mobile devices.

Local MPS standalone computers are designated as either 'overt' or 'covert' computer workstations for the purposes of Internet and social media access. You do need to be clear about the differences and restrictions regarding the two types of standalone computers, which are explained in the section on accessing the Internet.

Distinct MPS social media accounts are to be set up and maintained for community engagement and communication purposes; which **must** be kept separate from those used for intelligence, investigation purposes or other operational use. For advice on using social media accounts for intelligence gathering or investigation purposes you should follow the guidance at Met Operations and Intelligence Services - Online and Open Source Guidance

WARNING: You **must not** make *any* personal use of crime or intelligence systems [CRIS, CRIMINT, Merlin etc.] or any national police systems, such as the Police National Computer (PNC).

Unauthorised access to and use of police crime and intelligence systems or national police systems and the information contained thereon is a breach of the discipline code/ regulations and may also constitute a criminal offence. If individuals are in any doubt as to whether or not they may access a website or service they must initially verify this through their line manager or supervisor.

ACCESSING THE INTERNET

MPS users are able to access the Internet in several ways; the main ways are as follows:

AWARE FOUNDATION AND OTHER MPS NETWORKS

MPS personnel and other authorised persons have now been granted full access to the Internet both in an MPS business capacity and for personal use.

Business Use

- The Internet via AWARE Foundation is the medium to be used for work related activity such as general web browsing and overt research etc. A list of useful 'web links' is already provided on the Intranet homepage [under resources] to help the average user in their policing role - see MPS web links
- **Please note** that accessing the Internet through either an AWARE Foundation workstation or from an overt (non-AWARE) standalone workstation is **not** allowed for in-depth intelligence gathering, investigative, or other covert operational use **under any circumstances**.

- It should be noted that the work of the Police Federation, staff associations, the trade unions and any communication relating to union business is permitted and is interpreted under the heading of business use. This is provided that the use of the Internet and social media is limited to the organisation's core business and not for advertising, politically affiliated or other non-core activities. These organisations do need to be aware that privacy cannot be guaranteed for communications and files on MPS equipment

Personal Use

This is enabled through the MPS ICT infrastructure [i.e. AWARE Foundation], laptops and standalone computers. But you **must** note this strictly **excludes** any standalones specifically designated for covert investigations and intelligence work.

There is a clear expectation of trust placed on individuals to undertake any personal use of the Internet responsibly, appropriately, professionally and to follow instructions and guidance in this document and rules in the Use of MPS Information and ICT Systems Toolkit - Personal and Acceptable Use of MPS ICT Systems - Frequently Asked Questions (FAQs). Individual users are also required to meet any local management work requirements and line managers are to actively supervise their staff to ensure such compliance.

It is a line management responsibility to positively task individual staff and ensure appropriate use of the internet and social media by them, whether in an official business or personal capacity. The definition of what constitutes personal use and the conditions pertaining to personal use are outlined in the Use of MPS Information & ICT Systems Policy Toolkit - Personal and Acceptable Use of MPS ICT Systems - FAQs.

OVERT STAND-ALONE [Non-AWARE] INTERNET WORKSTATIONS

Only where there is a genuine business requirement that cannot be met via AWARE Foundation, will the use of overt stand-alone computers be permitted. They may be used for some business online transactions/ purchasing and other specialised activities over the Internet that (B)OCUs will need to justify cannot be undertaken on standard AWARE workstations.

Please note:

- *Only ACPO approved Level 1 Open Source Intelligence/ research should be carried out on overt devices that are attributable to the Police Service*
- *Overt stand-alone workstations are **not suitable** for covert investigative operational use or intelligence gathering at ACPO approved Levels 2 - 5 under any circumstances.*
- *Any Non-AWARE Foundation networks [i.e. local systems] that are intended to process MPS Information **must** be security assured or accredited by the Information Assurance Unit (IAU), Met HQ, before they can be connected to the Internet or social media. For*

the details of the process involved initially send an email with full system/ computer and contact details to DoI Mailbox - ISAT.

All (B)OCUs need to be aware that overt stand-alone Internet workstations **must** be managed in accordance with the following criteria, in order to enable the MPS to comply with its legal requirements and protect the system, plus any information held on it, from compromise;

1) Your (B)OCU commander/ head of branch **must** authorise any standalone connection to the Internet and for social media use. This is to ensure that there is a genuine business benefit that outweighs any security risk.

2) The (B)OCU commander/ head of branch must nominate a manager of usually Inspector/ Band C or equivalent level, to take responsibility for the workstation. The nominee will produce Security Operating Procedures (SyOPs) and manage the stand-alone, to ensure compliance with the locally written SyOPs and this guidance document.

3) The nominated manager will also be accountable for ensuring that system software is properly configured and for managing user accounts in accordance with **Expected Behaviour when using MPS ICT Systems** section [page 9] of the METSEC Code. The manager may delegate these activities to a nominated individual, however they remain accountable.

4) New users must be asked to read and sign their agreement to the SyOPs, and have read the MPS Information Code of Conduct v4.1 dated June 2013 before they are given access for the first time. Line management should retain any signed agreements.

5) **Under no circumstances** must any protectively marked information or personal data be held or processed on the stand-alone workstation. Information about security assurance/ accreditation and for producing SyOPs can be obtained from the Met HQ Information Assurance Unit (IAU) via the security advice mailbox or on telephone extension 78-5084.

As a user, you are accountable for any actions attributable to your use of a standalone computer. You are expected to comply with any access controls [such as logins and secure passwords]. In order to prevent unauthorised access when connected to the Internet or social media, you **must not** leave the stand-alone computer logged on and unattended outside of your control. This also applies to logging out of social media accounts/ applications.

COVERT STAND-ALONE [Non-AWARE] INTERNET WORKSTATIONS

Covert workstations are designed to facilitate operational activity such as investigations and intelligence gathering and **must only** be used for those purposes.

The minimum standards for investigation and research over the Internet and social media is set by SC&O39 Covert Governance and Intelligence Compliance and **must** be followed at all times. ***This is a matter of public and officer safety and is also required to assure the integrity of criminal investigations and intelligence gathering***:

- Under no circumstances should any other method of Internet and social media access be used for such purposes

- In addition, a covert workstation **must** only ever be used for covert work; otherwise its covert status, and potentially that of other ongoing police operations, will be permanently compromised

- Covert workstations are built to a specification that ensures that no trace of MPS activity is apparent to other Internet users, and no trace of an MPS electronic 'footprint' is left

Investigations & Intelligence Gathering - Guidance on the Covert Use of the Internet from Covert Workstations for Open Source Research & Investigation

Law enforcement agencies need to conduct regular and extensive research and investigation into intelligence that can now be found on the Internet. The sources of this intelligence can be many/ varied and could include the monitoring of various social media sites. Research and Investigation over the Internet particularly when carried out covertly does bring with it additional risks. It is therefore necessary for officers conducting this type of activity to work within standard guidelines.

First of all it is crucial to understand that by accessing any website from an overt system [such as AWARE] means an electronic 'footprint' will be recorded by the server on which the website is hosted. This has the effect of alerting anyone with access to the server to the fact that the website is of interest to police. There is then a risk that this would jeopardise important ongoing investigations or intelligence gathering operations, some of which you may not even be aware of [e.g. for example being carried out by other departments, police forces, crime enforcement agencies or the security services].

- As a consequence, investigation, intelligence gathering, research or other operational activities on the Internet [classified at ACPO approved levels 2 - 5] **must only** ever be conducted on a covert Internet workstation. This covers all instances where an investigator would not wish for those being investigated to be aware of the investigation or of police interest.

- Therefore equipment [i.e. designated covert workstations] **must** be used as their build means they cannot be attributed to the police service or any individual member of staff.

- Under no circumstances **must** you conduct such operational activity via the AWARE Foundation system, from an overt stand-alone workstation or any personal device [whether MPS or privately owned].

Covert Internet workstations exist in Borough Intelligence Units (BIU) and some other operational environments. You should seek out the assistance of trained Internet investigators responsible for your business area. Periodically Internet Investigations training sessions are organised centrally [MIB, SO15 etc.] relevant for officers and staff from investigations/ intelligence units, as well as MISPER teams/ response staff.

At a national police level accredited training courses [Level 1 Open Source Awareness Course] relies on officers/ staff having completed the following NCALT training packages:

- Communications Data in Investigations
- MoPI Management of Police Information
- Human Rights Act 1998
- Introduction to CPIA Criminal Proceedings Investigations Act 1996 disclosure; and
- RIPA Regulation of Investigatory Powers Act 2000 (RIPA)

If you are still unable or unqualified to access a covert workstation you should contact the MIB Open Source Guidance who may be able to carry out the work on your behalf and provide any necessary advice relevant to your enquiry. MIB provide detailed guidance on how open source Internet and social media investigations are to be conducted and the resources available.

Those with a requirement to go one step further and interact covertly with other Internet and social media users **must** exercise extreme caution. Such activities **must** be conducted lawfully, in compliance with RIPA, which covers surveillance and interception of communications activities. It is a minimum requirement that only officers who have completed the Covert Internet Investigators (CII) course [which includes RIPA], run by the College of Policing, may engage in such activity.

Covert Human Intelligence Source (CHIS) authorities are usually required prior to commencement. The Office of the Surveillance Commissioners/ ACPO advises that the police can set up and use 'false personas' on the Internet/ social media for a covert purpose; but **must** seek prior authorisation to do so, as such activity could otherwise be deemed unlawful and result in failed prosecutions. If officers go ahead and use social media to find suspects [without reference to covert policing standards], there is a real risk the defence will similarly use the same techniques to locate officers and then try to discredit them in court.

Also, MPS Officers and Staff must not conduct any criminal investigation research or intelligence activity over the internet or via a social media account from any personal devices. As this will leave an identifiable footprint on the internet it poses a real risk to the safety of the officer/ staff member and possibly others.

Guidelines have been issued by SC&O39 Covert Governance and Intelligence Compliance and cover nationally agreed levels of activity when carrying out online covert research and investigation across the Internet/ social media. The guidelines can be found on the intranet web pages for SC&O39 Covert Governance and Intelligence Compliance [and via MIB web pages] via link - Met Operations and Intelligence Services - Online and Open Source Guidance.

Additional guidance on identification evidence gathering from social media images [e.g. Facebook] was published on 11 September 2013 see - TP Criminal Justice Central Forensic Image Team VIIDO Guidance on Identifications from Social Media

SMART PHONES – The AWARE 'BLACKBERRY' EOM Mobile Device

Some AWARE users with particular business needs for mobile access are issued with a corporate smart phone. The smart phone currently used by the MPS is the AWARE Blackberry Email on the Move (EOM) device; which provides access to AWARE email and calendar, the MPS Intranet and other browser based services, including the Internet and social media.

Internet access on this device is routed through the Secure External Gateway (SEG) and the service/ restrictions are identical to those on other such systems [e.g. AWARE]; so rules with regard to usage of the Internet and conduct are also the same. In particular, you must exercise greater care when browsing the MPS Intranet when in public locations to ensure that you cannot be overlooked by strangers, as this may compromise MPS information or operations. Personal devices **must not** be used for investigation or research over the Internet as previously described.

The Acceptable Use of AWARE Blackberry EOM Devices SyOPs can be found on the MPS Digital Policing Intranet site.

WIRELESS APPLICATION PROTOCOL (WAP) MOBILE PHONES

Some users may possess other mobile phone handsets for MPS business purposes. Most modern mobile phones have the facility to access the Internet and social media, although access in such circumstances is over the mobile phone wireless network itself, not via the SEG. Unlike the AWARE Blackberry such devices cannot access services provided by the AWARE system.

The rules with regard to accessing the Internet and social media from AWARE Foundation, apply equally to all MPS supplied mobile devices. Authorised users need to be aware that such mobile devices will be audited and monitored to the same degree as other MPS communications and information systems. Users should understand that their personal conduct using MPS mobile devices is still subject to scrutiny and the discipline code. Personal devices **must not** be used for investigation or research over the Internet.

Please note - The loss, theft or compromise of any mobile device is a reportable security incident under the Security Incident Reporting Scheme. For further information management and information security advice for all forms of mobility go to Mobile Computing Security Guidance

THE USE OF SOCIAL MEDIA [SOCIAL NETWORKING]

Introduction

This is a growing area of communication and sharing technology, which has quickly been adopted by many organisations including the MPS and is used to communicate with partners and customers by setting up a presence on social networks or related web sites. The rapid expansion of social media technologies, such as Twitter, Flickr, LinkedIn and Facebook, presents the MPS with unique opportunities to engage and have constructive 2-way dialogues

with a wider range of people and communities with clear benefits in support of Total Policing. The Communications & Engagement Social Media Board will set the strategy and agenda for the productive use of social media. The MPS vision for using social media positively to improve communications is detailed through the following Intranet pages:

DMC Digital and Social Media Team and Toolkit

The term 'social media' refers to web-logs or blogs, micro blogs [e.g. Twitter], forums, sharing [e.g. YouTube and Flickr], social networks [e.g. Facebook and Twitter] and other related websites.

Expected Standards of behaviour - It should be appreciated that the principles and standards of behaviour covering the use of social media by MPS personnel and authorised persons [either in an official business or personal capacity] are broadly the same as those that apply to any other media. It should be remembered that social media is essentially a public forum so the same considerations apply as one would use, for example, if one was speaking at a public meeting or writing something for publication.

Officers and staff should always exercise care when using social media websites, whether for business or personal purposes and follow this guidance document and the Use of MPS Information & ICT Systems Policy Toolkit. As social media is an interactive medium it is expected that MPS personnel comply with core values, principles and particularly requirements relating to professionalism [i.e. integrity, honesty, objectivity and impartiality].

Social media is by its nature a public forum, open to scrutiny with minimal privacy controls. If you are online you are on the record as everything on the Internet is public and searchable. It should be expected that access to social media websites will be monitored at the SEG [at least automatically for 'traffic'] and by the Directorate of Professional Standards (DPS) in respect of behaviour in order to ensure compliance with this Guidance document.

Social media as part of the communications strategy - Social media should never be the only communications channel the MPS uses to contact the public. Remember that many vulnerable individuals or disadvantaged groups in the community may not yet have ready access to computer services, an important factor which needs to be considered in advance of any communications campaign. Social media is just another communication tool we can utilise to engage and interact with the communities we serve and to be most effective should always be used as part of a wider communications strategy.

Dealing with information requests received via social media - Social media is a medium used to request information about public services so all MPS personnel need to understand how such requests should be handled. Therefore, requests for information under the Freedom of Information Act 2000 (FoIA)/ Environmental Information Regulations 2004 (EIR) or subject access requests under the Data Protection Act 1998 (DPA) received via social media accounts **must** follow usual procedures and be referred promptly [within statutory time limits] to the Met HQ Information Services - Public Access Office (PAO) to be logged and processed. The PAO can advise on information requests and questions submitted via Twitter and Facebook.

USING SOCIAL MEDIA, ETC. FOR MPS BUSINESS PURPOSES

Introduction

All MPS personnel and other authorised persons are now permitted access to social media sites in furtherance of official business requirements, for example to communicate with the general public, specific communities/ organisations or individual citizens. It should be noted that access to some social media sites via AWARE may continue to be automatically blocked at the Secure External Gateway (SEG) on the grounds of recognised technical, security or other business reasons. Applications, however, can be made for access to social media sites and for the block to be removed if there is a clear business benefit.

Expected Standards of behaviour - Unless a business need dictates otherwise [and you may be asked to justify your actions], your personal conduct must remain in accordance with the instructions, principles and guidance described in this document and the instructions in the Use of MPS Information & ICT Systems Policy Toolkit.

Setting up social media accounts - The DMC Digital and Social Media Team and Toolkit sets out current social media channels and provides detailed guidance on their usage. Each (B)OCU Commander should appoint a (B)OCU Social Media Team Leader to control the business use of social media and ensure consistent communication feeds are maintained with local communities.

Should you have a requirement to set up and maintain a MPS web page, a social media account or a new web application, for example to reflect the work of a local unit, you must initially contact the Digital Policing - Digital Services Team. The Digital Policing - Digital Services team are responsible for the development and maintenance of Intranet, Internet, and Extranet publishing services for the MPS. Digital Policing - Digital Services will in some cases need to liaise with the Directorate of Media & Communications (DMC), as DMC must be consulted with regard to any requirement to publish MPS information into the public domain.

It should be noted that any new web applications **must** also undergo a security assurance process that meets the requirements of Met HQ Information Assurance Unit (IAU). You can contact the IAU through the DoI Mailbox - ISAT or on Tel ext. 78-5084.

Intelligence and Investigations using social media - Increasingly there is a legitimate business need for officers and staff to access social media websites in the course of crime investigations and for intelligence research/ evidence gathering purposes. In respect of both overt /covert open source intelligence research and investigation through social media, officers/ staff **must** follow the standards described in the section on accessing the Internet and instructions in the Use of MPS Information & ICT Systems Policy Toolkit.

USING SOCIAL MEDIA IN A PERSONAL CAPACITY

All MPS personnel and other authorised persons are now permitted to access social media sites for personal purposes from specified MPS ICT systems and equipment.

Personal Use of Social Media at work [i.e. on duty]
There is a clear expectation of trust placed on individuals to use social media responsibly, appropriately, professionally and to follow this guidance document and the instructions at Use of MPS Information & ICT Systems Policy Toolkit.

Operational safety - This aspect is particularly important to bear in mind away from the office during active operations when officers and staff need to be focused on the job in hand. There is also the possibility during some sensitive operations that organised criminals will use scanning equipment to pick up wireless traffic in the locality, so 'radio silence' should be applied. Therefore to minimise risks for the safety of yourself and others you should routinely check with your line manager to see if tweeting, using facebook etc. from a personal device is appropriate during a particular period of duty. Line managers have a direct responsibility to use their judgement to ensure sensible direction/ guidance and enforce compliance for the safety of their staff.

Personal Use of Social Media away from work [i.e. when off duty]
The MPS recognises that some users wish to engage in these activities in their own time, using their own equipment. If you do then be advised that, whilst there is no intention to restrict any reasonable exercise of your rights and freedoms, it is expected that you will conduct yourself in such a way as to avoid bringing the MPS into disrepute or compromising its effectiveness or the security of its operations or assets.

Personal identity, safety and reputation - It is in your own interests to recognise that there are some risks to individuals in accessing social media, particularly if security safeguards are not followed. For police officers [and possibly some police staff] there may be future career implications to be considered and understood in publicising your association with the MPS. It needs to be recognised that by engaging in activities such as posting information about yourself on the Internet [with or without images] you may no longer be eligible for appointment to certain covert/ sensitive operational posts within the MPS or other police/ security services. It may also affect your vetting status and ability to give evidence in court. You are therefore encouraged to discuss any concerns in this regard with your line manager.

Basic guidance on personal social media use - The following basic guidance applies to using social media websites in a personal capacity:

1. In full accordance with the MPS Equality Policy Toolkit and instructions in the Use of MPS Information & ICT Systems Policy Toolkit - Prohibited Use of ICT Systems Checklist, you **must not** display offensive images or make offensive comments, or in any way harass, intimidate, bully, victimise or discriminate against others, which could constitute a criminal offence and/ or lead to civil proceedings [such as defamation] against you. Any posting or other publication [including social media] which is defamatory in nature may result in personal liability, for which the MPS will not provide any indemnity and you should note that such a liability could also arise if comments are re-published by the media or others. Disciplinary proceedings will also be considered

for any member of staff involved as such behaviour is likely to threaten the reputation of the MPS.

2. You **must not** divulge any official MPS information, including personal data or information obtained through your work for the MPS, nor expand upon MPS information already available in the public domain. You must never reveal any protectively marked information [see the METSEC Code].

3. To reduce spam, phishing, and denial of service attacks you **must not** publish your or another's MPS email address on social media websites that you use in a personal capacity.

4. You **must not** use any MPS logo or other copyrighted material without permission. Respect the intellectual property rights of third parties and if in doubt seek advice. For further details please refer to the METSEC Code.

5. If you disclose that you work for the MPS, then you **must** make it absolutely clear that any views expressed are yours alone and do not represent the official position of the MPS.

Further protective measures - You may consider the following measures to protect your job/ role identity and reputation:

6. Whilst it is ultimately your decision, for your own security, it is suggested that you do not disclose your position as an MPS employee or officer. Whatever you decide, you should avoid disclosing any personal details which may be used for identity theft, or to identify your home address, or other sensitive details about yourself or your family. Do ensure that you make use of the privacy settings available on social networking sites.

7. If you do disclose your association with the MPS, you must consider whether it is appropriate to discuss your role within the MPS. You must never divulge any information that may compromise police operations or investigations or which breaches the Official Secrets Acts or the Data Protection Act 1998. **Never** reveal the security clearances [vetting levels] of either yourself or that of other police service personnel.

8. Irrespective of whether you disclose your position, you must do nothing which risks bringing the MPS into disrepute or compromising its effectiveness or the security of its operations or assets. To do otherwise might lead to disciplinary and/ or legal action, with potentially serious consequences for yourself and the organisation.

9. Regularly review the content of both your work and personal on-line profiles; so see the valuable advice at **Section 8 - Keeping your private life private** [page 7] of the ACPO Guidelines on Safe use of the Internet & Social Media January 2013

10. You may accept payment or other inducement for your own material produced away from your MPS employment, provided that this has been officially registered and sanctioned as a business interest, plus providing the material does not in any way relate to policing. Failure to register and obtain a sanction for a business interest may result in formal disciplinary action being taken. Information on how to register a business interest can be found in the Business Interests, Secondary Employment & Political Activities SOPs.

USEFUL TIPS FOR USING SOCIAL MEDIA IN A PROFESSIONAL MANNER

See Use of MPS Information & ICT Systems Policy Toolkit - Using Social Media for Professional Reasons Checklist.

MPS INTERNET SECURITY

The nature of the Internet - It should be realised that the Internet is fundamentally a vast unregulated electronic network that operates freely across international boundaries. The Internet has little if any in-built security or governance. As a result all MPS personnel and other persons authorised to access the Internet are required to have a basic understanding of the potential risks relating to access, take account of the guidance/ tips on how to remain secure online and help to protect identities.

Risks to email - Users need to have some basic understanding of the nature and risks relating to email which is only briefly mentioned within this Guidance document, so for more instructions and advice go to Use of MPS Information & ICT Systems Policy Toolkit and also The METSEC Code.

Web browsing and downloading also exposes a computer to risk. Consequently, there is a potential risk to any computer system connected to the Internet, and to any data held on it.

External risks to Computers - To summarise the primary dangers you need to be aware of include:

- **Information leakage**, meaning the unauthorised release of sensitive MPS information, whether unwittingly or maliciously, which has left the system and fallen into the wrong hands
- **Hacking**, which is the accessing of a computer program or data without authorisation [illegal activity under the Computer Misuse Act 1990 as amended]
- **Malicious software** [also known as Malware], such as Viruses, Worms and Trojans, introduced when web sites are visited and emails opened that contain attachments that are infected
- **Malicious attacks**, such as denial of service attacks, where the attacker can prevent a system from functioning efficiently or at all
- **Fraud**, such as identity theft e.g. through ‘phishing’ or ‘spear phishing’ [pronounced as ‘fishing’] attacks; where the fraudster sends emails designed to persuade recipients to disclose personal information. This is known as ‘social engineering’ and is a growing threat, not only for individuals, but also for organisations and their ICT systems
- **Risks to the MPS reputation** caused by the publication of incorrect, inappropriate or conflicting information that can create serious risks for the reputation of the MPS [e.g. through emails, unapproved news releases and social media based communications]

SECURE EXTERNAL GATEWAY (SEG) RESTRICTIONS

The Secure External Gateway (SEG)

The SEG protects the MPS technical infrastructure, systems and information by minimising risks and allows the MPS to provide users with relatively safe external email, web browsing and social media facilities through their AWARE workstation, AWARE laptop or MPS Blackberry EOM device.

The SEG works in the background and you will not usually be aware of the protection that it provides. However, you may find that certain incoming or outgoing emails will be blocked and you might be denied access to certain pages/ file types on the Internet. In most cases this will be the SEG doing what it was designed to do; preventing information leakage and the download of dangerous or suspicious code, blocking emails with potentially unacceptable content, or preventing users from browsing material the MPS deems unsuitable for access from its ICT equipment.

Despite technical controls to manage the constant stream of electronic [also known as cyber] threats, management of the SEG is reliant on all users being vigilant regarding such threats. Users should therefore only access the Internet and social media sites in a safe and responsible manner in accordance with this guidance document and Use of MPS Information & ICT Systems Policy Toolkit. Go to the Digital Policing - Secure Services MPS Web marshal FAQs for further guidance.

Blocked Access

If you need to gain access to a blocked web site for business purposes you should contact 'Gateway - DoI' who will consider your requirement. You may need your line management to support or approve any access.

Internet & Social Media sites blocked by the SEG

Although MPS personnel and authorised persons have been granted full Internet access, users will continue to find that their access is not completely unrestricted and that the SEG will continue to block some web sites. This is because the blocking of access to certain sites needs to be maintained to protect the MPS ICT infrastructure and for a range of technical, operational, risks to the MPS reputation, security and legal reasons. The SEG will therefore continue to automatically block:

- **Web mails and forums** [a variety of personal web mail accessible through sites such as gmail, hotmail etc., including some academic sites]
- **Video Streaming** [due to a lack of appropriate bandwith, except limited approved business access e.g. for NCALT e-Learning]
- **Other material** such as pornography and gambling web sites

When this occurs an explanatory message will appear on your screen. If you still need access you will have to initially contact Digital Policing - Secure Services giving your reasons

why the blocked web site should be opened up. You should be aware that attempts to access blocked sites is recorded and may be audited.

Download limitations

You may download material that you require in order to carry out your current duties. However, owing to the lack of appropriate bandwidth large downloads [other than those critical for the MPS business] may not be possible over AWARE Foundation. Downloads are blocked or access refused in order to protect the MPS infrastructure. Therefore sound, music, video, active code, executable files and electronic games will in general continue to be blocked, by default, at the MPS firewall [i.e. the SEG].

If that happens you may request that the SEG Administrator at Digital Policing - Secure Services releases certain files to you, provided that you can demonstrate a justifiable business requirement, backed by you line manager. Regular searches of MPS systems are conducted for such file types and those persons found to have saved them without an authorised business need will be required to justify their actions.

No software downloads onto desktops

Unlicensed software, shareware and similar freeware is often unreliable, poorly coded and may even contain malicious code. It also needs to be appreciated that some shareware might be free for individuals but not necessarily for commercial or corporate use. It is often the case that large organisations will have to pay and require licence(s) to use and operate it. For these reasons such software is strictly prohibited. Service instructions relating to software can be found in the **Expected Behaviour when using MPS ICT Systems** section [page 9] of the METSEC Code.

Secure encrypted on-line Internet sessions

Secure online sessions may be permitted for personal use, such as Internet banking and other online transactions but is subject to the following provisos. For the purpose of this guidance document, an online transaction is defined as ‘where the user must log in to a web site securely in order to access information or do business, such as purchasing goods and services’. In these circumstances AWARE Foundation only acts as the conduit or portal for the exchange of information via the secure sessions.

Secure online Internet sessions are commonly used as a secure method of communication in banking and by online shopping sites. This method prevents the interception and compromise of customer information, such as bank account and credit/ debit card details. The MPS has taken all reasonable steps to ensure the security of transactions over the Internet and the SEG and it is not configured to break the encryption or read the content of secure online Internet sessions. However, the MPS ICT infrastructure is subject to legitimate monitoring and as a result users should expect that the frequency [or ‘traffic’] of their access and sessions is recorded automatically.

As a consequence the MPS cannot guarantee complete privacy for users who choose to do online banking or online shopping via MPS systems. Your bank, for instance, may not accept that your online banking transactions in such circumstances are ‘private’ or meet banking

industry certification/ accreditation requirements or their particular banking terms/ conditions. Users who have concerns in this regard might wish to continue to access such secure online services through their home computer or personal device rather than via MPS equipment.

As a result users need to be clear that the MPS cannot accept any responsibility for any consequent difficulties or losses incurred. To make users fully aware of such limitations the following type of pop-up notice will appear whenever you try to access channels [as with this example relating to personal banking] via the Internet:

> '*You should understand that any personal on-line secure [encrypted] sessions that you engage in through the Internet is done in your personal capacity and is thereby undertaken at your own risk. Additionally no claims or guarantees are made that such sessions can be successfully completed accessing the Internet via AWARE Foundation. If you choose to engage in on-line banking you are solely responsible for meeting your banks terms or conditions over such transactions and any statutory or other requirements of the banking industry. The MPS/ MOPAC accepts no liability for any loss or damage however incurred [economic or otherwise], or in respect of any compromise of your personal data or identity.*'

Go to Digital Policing - Secure Services MPS Web marshal FAQs for further details on Internet access.

MONITORING INTERNET & SOCIAL MEDIA USE

Monitoring of Systems & Expectation of Privacy Statement - As part of the proper management of the MPS, its public functions and its resources, MPS ICT systems [including email, mobile, desktop and airwave/ telephony] are monitored to the extent permitted by law. For further details on the extent of such monitoring and users expectation of privacy should go to the Use of MPS Information & ICT Systems Policy Toolkit.

NB: If you choose to use MPS information and communication systems for personal reasons, you are giving implicit consent that your personal activity can be monitored and recorded. In this respect MPS personnel etc. who wish to ensure that their personal communications always remain private are advised to use their own personal/ home ICT equipment away from MPS premises.

FURTHER INFORMATION

Contact details and further information can be found at MPS Information & ICT Systems Policy Toolkit.

For further enquiries regarding this guidance document you can also contact the Information Assurance Unit (IAU), Met HQ, on internal telephone extension 78-5084 or via the security advice mailbox.

For further guidance on how to secure your home computer, other personally owned ICT equipment and to keep your online life secure, consider the excellent independent advice to be found at the Get Safe-On-Line website.