SEMPER VIGILO

POLICE
SCOTLAND
Keeping people safe

INTERNET, RESEARCH AND INVESTIGATIONS

Standard Operating Procedures

Notice:

This document has been made available through the Police Service of Scotland Freedom of Information Publication Scheme. It should not be utilised as guidance or instruction by any police officer or employee as it may have been redacted due to legal exemptions.

Owning Department:	**SCD- Intelligence Support**
Author / Reviewer:	**Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 30 Prejudice to effective conduct of public affairs.**
Version number:	1.00
Date Published:	25/07/2013
Due for review on:	23/06/2014
EIA Completed:	13/03/2013
ECHR compliant:	Yes
Data Protection compliant:	Yes
FOI compliant:	Yes
Health & Safety compliant:	Yes
GPMS compliant:	Yes
Records Management compliant:	Yes

CONTENTS

APPENDICES

1. PURPOSE

1.1 This Standard Operating Procedure (SOP) outlines what activity is appropriate with regard to accessing information on the internet to conduct research and investigation for a policing purpose.

1.2 The internet and in particular social media sites can be a rich source of intelligence and on occasion can provide information of significant evidential value. The Police Service of Scotland (PSoS) actively encourages its employees to make use of the internet when conducting their enquiries, whenever it is appropriate for them to do so.

1.3 A three tier model has been developed which identifies the various overt and covert techniques and identifies the level of authority and training etc that is required. The model will be explained in detail in Section 4 of this document.

1.4 The primary purpose of this SOP is to provide the necessary information to ensure officers are able to conduct internet enquiries, at an appropriate level, in a professional manner, without bringing adverse risk to PSoS or having evidence excluded from court.

1.5 This SOP does not cover overt community engagement through social media which is the remit of Corporate Communications.

2. INTERNET RESEARCH & INVESTIGATIONS

2.1 In the majority of cases, the most appropriate method for securing evidence or intelligence from social media sites, blogs and other online applications will be through Internet Investigations. Additionally, there is significant legislation which impacts on the way Law Enforcement Agencies are able to conduct enquiries using the internet.

2.2 Those conducting Internet Research & Investigations should be aware that on every occasion a computer accesses the internet it will leave a footprint. Providers of websites and applications can and will record the IP addresses of persons using their services. In the main part this is not a threat to Law Enforcement conducting overt enquiries as the information, if gathered, is mainly used for commercial purposes etc.

2.3 Less scrupulous website providers may use this information to identify Law Enforcement Officers who are conducting enquiries on overt Police computers.

2.4 Where there is good reason for the Police to be interested in the site concerned and no security has been overcome or falsehood used to enter the site this should not limit our investigations.

2.5 Investigators should be aware that where they are identified as a Law Enforcement employee by such a site, then the possibility of being provided misinformation can not be ruled out.

2.6 A Manual of Guidance provides more detailed direction on the conduct of Internet Investigations.

3. THREE TIER INTERNET RESEARCH & INVESTIGATIONS MODEL

3.1 The 3 tier model has been devised to provide structure and uniformity to online research and investigations. The tiers are identified at follows:

- Tier 1 – Overt Internet Research
- Tier 2 – Covert Internet Research
- Tier 3 – Covert Internet Investigations

3.2 TIER 1 – OVERT INTERNET RESEARCH

3.2.1 It is appropriate for all employees to access the Internet to complete the following tasks overtly:

- Check to see if a person has a social media account
- Establish a person or group’s Unique Identification Number
- View public profiles or groups to secure evidence or intelligence
- Request the removal of offensive material
- Use the internet as an overt method of communication. (This strategy must be approved by the Senior Investigating Officer or other senior responsible officer.)

3.2.2 There should be no covert nature to Overt Internet Research. All accounts used for searching at Tier 1 must clearly indicate they are being utilised for a policing purpose.

3.2.3 It should be noted that the systematic monitoring a personal profile, even where the profile is open and an overt Police account is used, will be considered to be directed surveillance, if it is not clear to the subject that such activity is taking place. Due to the requirement for RIPA authorisation this activity will fall within Tier 2 outlined below.

3.2.4 Certain restrictions on the corporate web browser may mean that overt searches will need to be carried out on a standalone computer with internet access.

3.2.5 There will no activity at Tier 1 which requires authorisation in terms Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A).

3.3 TIER 2 - COVERT INTERNET RESEARCH

3.3.1 Covert Internet Research will only be conducted by personnel within Internet Investigation Units (or authorised departments) who have received specialist training and have access to covert computers and software that are independent of the Police National Network (PNN). Only these personnel have been authorised to conduct more complex covert internet enquiries including using a pseudonym to:

- View closed profiles to secure evidence or intelligence
- Join and monitor closed groups
- Monitor open or closed Facebook accounts

3.3.2 As mentioned in paragraph 3.2.3 above; the systematic monitoring a personal profile, even where the profile is open and an overt Police account is used, will be considered to be directed surveillance, if it is not clear to the subject that such activity is taking place. Due to the requirement for RIPA Authorisation this activity will fall within Tier 2.

3.3.3 Tier 2 research will almost certainly require a Direct Surveillance Authority in terms of RIP(S)A.

3.4 TIER 3 - COVERT INTERNET INVESTIGATIONS

3.4.1 Covert Internet Investigations will only be conducted by personnel within Internet Investigation Unit who are nationally Accredited Covert Internet Investigators and equipped to conduct covert interaction on the internet. This is a sensitive policing tactic that will only be utilised in serious cases. Operatives can be deployed on the internet to:

- Conduct “Covert Internet Research” as at 3.3 above
- Interact with other internet users by means of a pseudonym
- Authorised interaction

3.4.2 Tier 3 activity will require Use and Conduct authority in terms of RIP(S)A.

4. ACCOUNT TAKEOVERS

4.1 Where a complainer, suspect or witness provides details of a username and password to a social media or other similar account access can only be gained when the appropriate RIP(S)A authorities are in place.

4.2 This activity must only be conducted by personnel who are trained to conduct activity under Tiers 2 or 3.

4.3 Written and informed permission of the account holder must be obtained prior to accessing accounts is this manner.

5. HARDWARE

5.1 There are currently three forms of computers installed within throughout the PSoS estate which are described as follows:

- PNN Computers
- Standalone Computers
- Covert Computers

5.2 PNN COMPUTERS

5.2.1 All police officers and police staff have access to the intranet through a personal login. This is facilitated by the Police National Network (PNN), a computer network which provides the Police and other government bodies with an ability to move data and communicate with some degree of security.

5.2.2 Access to the internet is facilitated through the PNN network utilising an internet connection delivered by a commercial Internet Service Provider (ISP). This internet connection is delivered using a static IP address which will resolve back to the individual police force or agency. Resolving these IP addresses is a simple task and can be done using open source tools.

5.2.3 PNN computers **must not be** used for Covert Internet Activity.

5.3 STANDALONE COMPUTERS

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 31 (1) (a) (b) National security and defence.

5.4 COVERT COMPUTERS

Information has been removed due to its content being exempt in terms of the Freedom of Information (Scotland) Act 2002, Section 31 (1) (a) (b) National security and defence.

6. EVIDENCE CAPTURE

6.1 Processes must be in place to fully record and capture the content of a webpage that may contain material that is of evidential value. This must be available at a later date for audit or examination.

6.2 Computer software to carry out these functions should be installed and available for use.

6.3 Further advice with regard to evidential capture can be obtained from the Internet Instigations Unit.

7. PERSONAL USE OF THE INTERNET & SOCIAL MEDIA SITES

7.1 Whilst this document is aimed at the use of the internet for a policing purpose, it is important to understand that, in order to protect the privacy of officers and maintain evidential and professional integrity, social media and internet accounts used for policing purposes must be separated from those used for personal social networking.

7.2 Whilst PSoS does not seek to prohibit its employees from using social media sites, it does require staff to be mindful of the following points:

- PSoS prohibits its employees from using IT Systems to access social media websites for personal / private use;
- Officers must not use their PSoS email address to register for any personal / private accounts;
- Officers must remember that the same obligations apply to social networking online as they do in every other aspects of your social life;
- You have a duty of confidentiality regarding work issues;
- You must not do anything that would bring discredit or disrepute to the Police Service;
- Social media websites are **not** private. Whilst you can apply some security settings to your profile, it is not possible to confirm how secure these might be. You should consider that when you post information or photos onto the Internet you have lost control of them and other people can do whatever they want with them;
- Defence legal teams, criminals, and journalists are all known to use the Internet to research police activity and find information about police employees. Do not disclose any information that has the potential to compromise you or your family’s safety, or cause you professional embarrassment.

7.3 Further information of the use of the internet and electronic communications can be found within the E-Mail and Internet Security SOP.

8. DISCLOSURE

8.1 All officers conducting Internet Research and Investigations must be aware of their obligations with regard to disclosure. All records of activity and captures made must be stored securely to allow revelation and disclosure at a later date, should this be required.

8.2 Further advice and practical guidance can found within the ACPOS, Disclosure in Criminal Proceedings, ‘A practical Guide’ and 'Disclosure of Evidence in Criminal Proceedings' SOP.

APPENDIX ‘I’

LIST OF ASSOCIATED LEGISLATION

- Human Rights Act 1998
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Computer Misuse Act 1990
- Data Protection Act 1998
- Police Act 1997
- Criminal Justice and Licensing (Scotland) Act 2010

APPENDIX ‘J’

LIST OF ASSOCIATED REFERENCE DOCUMENTS

- Internet Investigations Manual of Guidance
- ACPO Guidelines on the Safe Use of the Internet and Social Media by Police Officers and Police Staff
- Communications Data SOP
- Crime Investigation SOP
- Digitally Stored Evidence SOP
- Email and Internet Security SOP
- Indecent Images of Children on Digital Media SOP
- ACPOS, Disclosure in Criminal Proceedings, ‘A practical Guide’
- 'Disclosure of Evidence in Criminal Proceedings' SOP.

APPENDIX ‘L’

GLOSSARY OF TERMS

3g Dongle - A 3g Dongle is a device which operates over the cellular mobile telephony network and provides connectivity to the internet.

IP Address - An Internet Protocol Address is internet routing information. Each and every connection to the internet will have an allocated IP address which is unique at the time and date of issue. Where IP Address are capture for further enquiry it is imperative that the associated date and time (to the second) is also captured.

IP Footprint - An IP footprint will include the IP address being used It may also include additional information such as the type of device being used, software installed on that device, information held within the ‘clipboard’ of the device etc.