POLICY – Open Source and Social Media

Number: S 2800 **Date Published: 21 June 2019**

1.0 Summary of Changes

1.1 This policy has been updated due to changes in legislation and the introduction of the Internet Intelligence Investigation Unit (III team) formally known as open source following the SCD review.

1.2 The team will provide both proactive and re-active capabilities to support front line officers in a quest to tackle high harm crime within Essex Police and Kent Police. All staff should be aware of this policy, understand the legal implications and governance of open source enquiries and the security/data protection that underpins the investigative tactic.

1.3 This policy will affect all staff not just those within the III team. Compliance in terms of RIPA and national guidance is imperative to all staff involved in criminal investigations where consideration of open source tactics are sought.

Other changes made are:

- New paragraph 2.3 explaining the role of the III team;
- New paragraph 2.4 giving the definition of internet intelligence and investigations;
- Within paragraph 3.2 the Investigatory Powers Act included, and advice where staff can see support;
- Within paragraph 3.4 clarity given re authorisation for investigation/research;
- Paragraph 3.7 updates the definition of open source;
- Paragraph 4.1.1 the III team has been added;
- Within the risk assessment section 4.2 amended/new paragraphs have been added:
    - 4.2.1, 4.2.2, 4.2.6, 4.2.8 and 4.2.9.
- New paragraphs added within section 7 regarding data security and retention and disposal of records;
- Author details updated.

2.0 What this Policy is About

2.1 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 reports).

2.2 Rapidly increasing use of the Internet and social networking sites across communities and businesses has resulted in law enforcement having access to an array of investigative tools. Social network sites (and other 'open source' intelligence resources) contain a wealth of information, intelligence and evidence about suspects, victims, witnesses, members of organised crime groups and other aspects of criminal and anti-social activity. Organised crime groups are frequently using social network to support their criminal enterprise. Those involved in offences against children utilise social media to target vulnerable children and share images and data of an indecent nature.

2.3 The III team will be the strategic lead for all open source investigative functions within Essex Police and Kent Police. They will ensure that only those trained appropriately will fulfil the role and ensure that staff act within the boundaries of the law. This will protect individuals, investigations and the organisations but provide a proactive tool to tackle organised crime. Compliance with this policy and any linked procedures is mandatory for the use of open source tactics within investigations.

2.4 National strategy defines Internet Intelligence & Investigations (III) as:

- The use of internet resources to gather information, intelligence and evidence. This includes but is not limited to, the use of overt and covert tactics to:
    - Access areas which would otherwise be closed;
    - Gather metadata on individuals' activity through deployment of online resources;
    - Monitor social media or other online activity of a group, individual or relevant geographical area.

Compliance with this policy and any linked procedures is mandatory.

3.0 Statement of Policy

3.1 It is vital that officers and staff of Essex Police and Kent Police who make use of information contained in social network, other open source sites and the Internet do so in a manner in accordance with the law. They must utilise an approach that achieves best evidence, protecting where necessary potentially sensitive police tactics and this policy applies to all persons engaged in open source investigation/research (OSIR) in order to maintain the integrity of any evidence gained and in order to avoid compromise of the following:

- The hardware/software infrastructure of police computer systems;
- Police tactics;
- Ongoing and future police operations;
- The personal safety of the individual;
- Reputational risks to the organisation.

3.2 The use of social network sites as an investigative tool has the potential to impact on individual's rights to privacy under Human Rights and may therefore require authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA) and or the Investigatory Powers Act 2016. If unsure staff should seek advice and support from the III team and or Force legal departments within Essex Police and Kent Police.

3.3 The Counter Terrorism and Security Act (CTSA) 2015 places a duty on various specified authorities to have 'due regard to the need to prevent people being drawn into terrorism'. This is referred to as a 'Prevent Duty' and involves:

- Responding to the ideological challenge of terrorism;
- Preventing people from being drawn into terrorism;
- Working with sectors and institutions where there are risks of radicalisation.

3.3.1 The CTSA 2015 also places a duty upon specified authorities in relation to supporting people vulnerable to being drawn into terrorism through the Channel programme. Channel is a multi-agency safeguarding programme, which provides support to those individuals who may be vulnerable to being drawn into any form of extremism that could lead to terrorist related activity.

3.3.2 This policy has been reviewed and assessed that the CTSA duties could be relevant and as such your attention is drawn to your responsibilities under the Act. Further details about the Prevent Duty and the Channel Duty can be found below.

- Learn more about the Prevent Duty;
- Learn more about the Channel Duty.

3.4 In addition prior to engaging in any open source investigation/research staff should have been authorised to undergo this tactic by their line management and with the express permission from the III team. Those involved in carrying this function should have a good understanding of the Legislation and Guidance that may apply, including:

- Human Rights Act 1998 (HRA);
- Computer Misuse Act 1980 (CMA);
- Data Protection Act 1998 (DPA);
- PACE 1984;
- Criminal Procedure and Investigations Act 1996 (CPIA);
- Police Act 1997;
- Management of Police Information 2010 (MoPI);
- NPCC principles for recovery of digital/computer data;
- Investigatory Powers Act 2016.

3.5 In addition consideration should be given to the ethical principles by reflecting on actions that may be permissible in terms of the law, but may not be ethically sound, including the values enshrined in the Code of Ethics.

3.6 Private Information is information relating to a person's private or family life. It should be taken generally to include any aspect of a person's private or personal relationship with others including professional and business relationships. Information on social media may still be regarded as private, and the subject has an expectation of privacy under Article 8 of the Human Rights Act whether or not access controls such as the 'friends' control in 'Facebook' have been activated.

3.7 Traditionally the ‘Open Source’ element of Internet Intelligence and Investigation also includes more traditional media within the public domain including books, journals, academic literature, news media and subscription databases some of which comprise both open and close source elements such as credit reference agencies, and people based databases such as GB Connexus and pure ‘Open Source’ ones such as company data bases and Land Registry for example. The new national strategy for Internet Intelligence and Investigation includes those which are delivered via internet based subscription services, but excludes non-internet traditional ‘Open Source’. However, the definition would cover news and other media discoverable on the internet via a search engine such as via Google Scholar for academic journals etc.

4.0 Implications of the Policy

4.1 Finance / Staffing / Training / Other

4.1.1 Staff carrying out any type of open source investigation/research over the Internet must be appropriately trained relevant to the level of use/intrusiveness they are conducting. For example; for all basic level one of open source research officers should have completed the NCALT Level One learning package. The III team will be responsible for the management and permission criteria for open source enquiries outside of the proactive and reactive III teams within SCD.

4.1.2 All open source activity conducted on mobile devices will be at level one, as per the current NPCC guidance, and will leave a police footprint. Therefore only basic open source should be conducted via mobile devices, although this may include social media. Consideration should always be given to the suitability of performing an open source check in this way in terms of the digital footprint left behind.

4.1.3 Level two open source searches will be largely done on un-attributable computers by intelligence and investigation officers and staff. Level three will be the preserve of the Open Source Unit. If in doubt contact the Unit for advice.

4.2 Risk Assessment(s)

4.2.1 This document does not cover overt community engagement through social media or Undercover Online (UCOL) authorised activity, both fall into the remit of separate capability leads.

4.2.2 Under ‘Core Internet Use’ individuals will not access areas of the internet which require a username and password. It is also important to remember that although Core Internet Use is overt and is effectively limited to information and data in the public domain this does not mean that the subject(s) of the data have given up all right to privacy, and Article 8 of the Human Rights Act does still have to be considered as does other legislation such as the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Protection Act and law Enforcement Directive 2018. All use of the internet for a policing purpose must also be ethical and in accordance with the policing Code of Ethics. If on consideration RIPA applies then the activity cannot be conducted as Overt III. If in doubt please refer to your force Internet Intelligence and Investigations Team.

4.2.3 Failure to adhere to these guidelines and its associated procedures will result in:

- Risk of serious reputational damage to the Force through inappropriate use;
- Risk of compromise to on-going investigations, sensitive police tactics and reduced opportunity to gather intelligence to solve crime;
- Breach of RIPA reportable to OSC and possible discipline issues;
- Lost opportunities to fully engage with the communities we serve, especially those in hard-to-reach groups.

4.2.4 Any activity carried out across the Internet leaves a trace or footprint that can identify the device used and, in some instances, the individual carrying out that activity. Staff engaged in investigation and/or research over the Internet must take precautions to protect the security of themselves and of police computer systems. Non-attributable computers must only be used for authorised open source investigation/research and never used for personal use.

4.2.5 However, open source is a powerful investigation and intelligence source and its exploitation is encouraged by all officers and staff.

4.2.6 No covert tactics will be used for Internet Intelligence & Investigations. Where a username and password is required to access an online space the credentials provided must reflect the fact that the account / profile is being utilised for a policing purpose and a record kept of all activity conducted. As with Core Internet Use please refer to your force Internet Intelligence and Investigations Team or Unit for advice if required.

4.2.7 Only Level 1 Open Source Intelligence/research (see SOP/procedure S2801) should be carried out on devices that are attributable to the Police Service. For any other type of covert investigation/research, where the investigator would not wish those being investigated to be aware of the investigation or of police interest, equipment must be used which cannot be attributed to the Police Service or any individual member of staff.

4.2.8 It should be noted that the systematic monitoring of 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 Regulation of Investigatory Powers Act 2000 (RIPA) authorisation this activity falls within Covert Internet Intelligence & Investigations.

4.2.9 All individuals conducting any online activity must be in a position to record, and bear witness to, any content which they observe. To this end no online activity should be conducted by individuals who are considered ‘firewalled’ from appearing at court.

4.3 Equality Impact Assessment

4.3.1 This policy has been assessed with regard to an Equality Impact Assessment. As a result of this assessment it has been graded as having a low potential impact as the proposals in this policy would have no potential or actual differential impact on grounds of age, sex, disability, race, religion or belief, marriage and civil partnership, sexual orientation, gender reassignment and pregnancy and maternity.

5.0 Consultation

5.1 The following have been consulted during the formulation of this document:

- IT Security
- PSD
- Equality and Diversity
- Health and Safety
- Legal Services
- HR
- Finance
- Estate
- IT Services
- Corporate Communications
- Unison
- Federation
- Superintendents Association
- Special Branch / IT
- PPU / LPA representatives
- CID / L&D
- Operational Policing Command

6.0 Monitoring and Review

6.1 This policy will be reviewed yearly to enable the changes and development in internet opportunities to be fully explored and considered.

7.0 Related force policies or related procedures (Essex) / linked standard operating procedures (Kent)

- **Joint** – S 2801 Procedure/SOP – Open Source and Social Media
- **Joint –** W 1001 Procedure/SOP – ICT Acceptable Use

7.1 Data Security

8.1.1 Essex Police and Kent Police have measures in place to protect the security of your data in accordance with our Information Management Policy – W1000 Policy – Information Management.

7.2 Retention & Disposal of Records

7.2.1 Essex Police and Kent Police will hold data in accordance with our Records Review, Retention & Disposal Policy – W 1012 Procedure/SOP - Records Review, Retention and Disposal.

7.2.2 We will only hold data for as long as necessary for the purposes for which we collected.

8.0 Other source documents, e.g. Legislation, APP, partnership agreements (if applicable)

- Prevent Duty;
- Channel Duty
- ACPO Guidance – NPCC Guidance on Open Source Investigation/Research