1.0 Summary of Changes

1.1 The policy has been reviewed in May 2017 and is subject to substantial revision as a consequence of the roll out of mobile devices across Kent and Essex providing mobile access to open source and social media. This revised procedure/SOP should be read by all police officers, police staff, Special Constables and volunteers who use open source, social networking and video sharing sites to assist in conducting investigations and/or intelligence research/development.

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. Information contained in such sites has the potential to impact upon many aspects of policing.

2.3 Compliance with this policy and any linked procedures is mandatory for the use of open source, including social media on both desk top and mobile devices.

Compliance with this policy and any linked procedures/SOPs 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 and may therefore require authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA).

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 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.

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.

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.

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 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.

4.2.2 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.
4.2.3 However, open source is a powerful investigation and intelligence source and its exploitation is encouraged by all officers and staff.

4.2.4 Any activity conducted across the Internet leaves a trace or footprint. Consideration should be given to whether your activity is classed as ‘covert’ in that you would not wish the subjects of the research or investigation to be aware of the activity. If it is covert, then equipment must be used that cannot be attributed, just as overt activity must be carried out on attributable equipment. Carrying out overt activity on covert equipment runs the risk of compromising the equipment as well as any operational activity which has been conducted on it.

4.2.5 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.

4.2.6 Access to Social Media via Mobile Devices

4.2.6.1 Access to social media via force mobile devices will leave a force footprint, and are therefore only suitable for Level One Open Source research. (See SOP/procedure S 2801).

4.2.6.2 Under no circumstances are personal mobile devices to be used for social media and Internet based open source research and enquiries. Such usage could put the officer or member of staff and their family at risk. Personal phones may be used for very general enquiries such as looking up locations, as long as this in itself is not sensitive, and should not include any addresses of locations which could compromise either operational security or the officer’s safety. If in doubt the approval of a supervisor should be sought.

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 were invited to provide feedback in the consultation phase during the formulation of this document:

- Essex Unison
- Essex Police Federation)
- Essex Equality and Diversity Co-ordinator
- Essex Special Branch
- Essex Health & Safety
- Essex Strategic Change Team
- Essex PSD Superintendent
- Essex Info Security
- Essex Data Protection
- Essex Superintendents Association
- Communities and Engagement Coordinator
- Joint IT
- Joint HR
- Joint finance
- Kent Media
- Kent Unison
- Kent Federation
- Kent H&S
- Kent Supts Association
- Kent Special Branch
- Kent Legal

6.0 Monitoring and Review

6.1 Due to the fast pace of change in the development of the internet and social network/ open source sites this policy will be reviewed every year. The review will be done by the policy author.

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
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