**NOT PROTECTIVELY MARKED**

**Published** | | Event History

## Policy owned by Investigative Services
## Internet Investigation

### 1. Policy Purpose and key drivers

The purpose of this policy and associated standard operating procedures are to provide a robust framework to govern the use of internet investigation techniques by Staffordshire Police. This includes all levels of open source research as well as more covert activities such as befriending and non CHIS online interaction .

The Standard Operating Practices linked to this policy give specific guidance and explain the procedures that should be adopted in relation to all aspects of internet investigation. They also provide a clear understanding of legislative position and outline the role of the Digital Intelligence Team who administer and provide oversight for internet investigation within Staffordshire Police .

### Key Drivers

- The rapid growth of digital technology , particularly the internet.
- The social networking revolution .
- Convergence of the internet and mobile technologies .
- Exploiting the internet as a source of intelligence and evidence .
- The need to police effectively in a digital age .
- The significant investment in Open Source training made by Staffordshire Police .
- Ensuring internet investigation is used effectively by Staffordshire Police to prevent and detect crime and protect vulnerable people .
- Ensure that Staffordshire Police conduct internet investigation ethically and lawfully.

### Background

The rapid growth of the internet and mobile technology has revolutionised the way we communicate and access information. These technologies are growing faster than anything before in the history of technology and have brought about the biggest social shift since the industrial revolution. The UK is one of the most internet engaged countries in the world and users spend more time online than any other European country. The UK is also at the forefront of using social networking sites (SNS) and accessing the internet using mobile devices via WiFi and 3G/4G connectivity. Whilst this constantly evolving technological landscape presents challenges to law enforcement it also offers new sources of evidence and intelligence, which can benefit all levels of policing. It is therefore essential that Staffordshire Police are in a position to exploit the investigative opportunities that the internet and other digital technology provides. With this in mind the Force has developed a comprehensive strategy designed to deliver a capability at all levels of internet investigation, which will put Staffordshire Police at the forefront nationally in this new and strategically important area of business .

The Force has made a significant investment in training staff from across the organisation to undertake open source investigation (OSI). It has also established the Digital Intelligence Team (DIT) which will be the central point of contact for providing tactical advice and guidance concerning the use of the internet and digital technologies for investigative purposes. Although the policy and procedures focus on OSI, as this will account for the vast majority of internet investigation work undertaken, they do outline procedures for higher levels of internet investigation which involve more covert tactics.

Whilst it is essential that investigators seek to exploit the internet as a source of evidence and intelligence, it is equally important that this is done in a way which is lawful, ethical and in accordance with relevant legislation and the Standards of Professional Behaviour (Police (Conduct) Regulations 2012 and Police Staff Council Joint Circular 54 to maintain public confidence and protect the reputation of the Force. The purpose of this policy and operating procedures is to provide the necessary governance to this area of business and give staff a clear procedural framework to adhere to when undertaking internet investigation.

This policy replaces the Using the Internet for Investigative Purposes – Interim Guidance issued in 2013. Its content has been agreed with Central Authorities Bureau (CAB), Anti-Corruption Unit, Information Security and Staff Associations. This guidance reflects ACPO Guidance for Online Research and Investigation and current OSC guidance for Covert Surveillance of Social Networking Sites (SNS). Staff engaging in any form of internet investigation must therefore comply with this policy. Failure to do so could result in disciplinary action being taken. Any member of staff who requires any form of clarification concerning this guidance should contact the DIT.

| **Related Documents** | |
|---|---|
| Links to related documents: | Internet Investigation - Covert Online Accounts (Procedure)<br>Internet Investigation - Covert Web Access (Procedure)<br>Internet Investigation - Examples (Procedure)<br>Internet Investigation - Incidents Involving Risk to Life (Procedure)<br>Internet Investigation - Joining Closed Groups on Social Networking Sites and Other Online Platforms (Procedure)<br>Internet Investigation - Levels of Internet Investigation & Definition of Open Source (Procedure)<br>Internet Investigation - Liking, Following & Befriending on Social Networking Sites (Procedure)<br>Internet Investigation - Open Source Evidence/Intelligence Gathering Procedures & RIPA (Procedure)<br>Internet Investigation - Use of Personal Devices and Online Accounts/Profiles (Procedure) |
| **Gatekeeper** - the Author suggested the following Procedure document(s) to link to. | Internet Investigation - Covert Online Accounts; Internet Investigation - Covert Online Interaction; Internet Investigation - Covert Web Access; Internet Investigation - Examples; Internet Investigation - Incidents Involving Risk to Life; Internet Investigation - Joining Closed Groups on Social Networking Sites and Other Online Platforms; Internet Investigation - Levels of Internet Investigation & Definition of Open Source; Internet Investigation - Liking, Following & Befriending on Social Networking Sites; Internet Investigation - Open Source Evidence/Intelligence Gathering Procedures & RIPA; Internet Investigation - Use of Personal Devices and Online Accounts/Profiles |

| Relevant Dates and Review Period | |
|---|---|
| Effective Date: | 04/01/2016 |
| Review Date: | 18/04/2018 |
| Review Frequency: | Annually |

| Policy Basis and Implications | |
|---|---|
| 2. Legal Basis: | Regulation of Investigatory Powers Act 2000 (RIPA) and associated Codes of Practice<br>Criminal Procedure and Investigations Act 1996 (CPIA) and associated Codes of Practice - covers the recording, preservation and disclosure of material obtained during a criminal investigation. (Failure to comply with the code may result in evidence being inadmissible) |
| 3. Management of Police Information (MoPI): | MoPI Policing Purpose:<br>Protecting Life and Property, Preventing the commission of offences, Bringing offenders to justice<br>MoPI Review, Retention and Disposal addressed as follows:<br>Officers engaged in this activity will be aware of disclosure and the RRD policy along with CPIA and DPA. |
| 4. Associated Benefits: | The success of this policy will be measured in terms of the lawful, ethical and effective use of internet investigation within Staffordshire. This in turn will enhance the ability of the Force to use internet investigation techniques to prevent and detect crime and protect local communities. |
| 5. Consultation: | This policy and associated standard operating procedures have been subject to a rigorous consultation process during the development phase. The Central Authorities Bureau, Learning & Development Dept and Anti Corruption Unit have played a central role in the drafting of the policy and procedures. Other groups and organisations that have been consulted or contacted in its formulation are:-<br>The Office Of Surveillance Commissioners<br>College of Policing<br>The Police Federation<br>Unison<br>Staffordshire Association for Women In Policing<br>Staffordshire Police Disability Support Group<br>Staffordshire Multicultural Association<br>Staffordshire Police Lesbian, Gay and Bi-Sexual Group |
| 6. Financial Implications: | The Policy continues to be implemented through existing funding. |
| 7. Human Resources / Training: | Open source internet investigation training forms part of the Learning & Development training plan and course material is reviewed and updated on an annual basis. Higher levels of internet invetigation training are delivered by the College of Policing. |
| 8. Associated Policy: | None |

| FOI, Human Rights and Equality Impact Assessment Indicators | | | |
|---|---|---|---|
| FOIA: | Release to Public | | |
| ECHR: | Compliant with proportionality test | Articles engaged: | Article 2 Right To Life; Article 6 Fair Trial; Article 8 Right to respect for Private and Family life |
| EIA: | Compliant | Compliant with Code of Ethics: | Yes |

| Indexing | |
|---|---|
| Categories: | Crime Investigation<br>Intelligence<br>Major Crime<br>Protecting Vulnerable People |

RIPA

**NOT PROTECTIVELY MARKED**