North Yorkshire County Council

Business and Environmental Services

Executive Members

11 December 2019

Covert Activity Policy

Report of the Assistant Director - Growth, Planning and Trading Standards

1.0 Purpose of the report

1.1 To review the Covert Activity Policy with the Corporate Director Business and Environmental Services (BES) and the BES Executive Members and seek continued approval for its use.

1.2 To report to BES Executive Members and the Corporate Director (BES) on the use made of the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and covert activity during October 2018 to September 2019.

2.0 Background to the Report

2.1 The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) provide a legal framework for the lawful interference with an individual's right to a private and family life under article 8 of the European Convention on Human Rights (ECHR) following the Convention's incorporation into UK law by the Human Rights Act 2000. The Acts allow local authorities to undertake covert activities within the legal framework provided that they are done solely for 'the prevention or detection of crime or disorder'. The Acts does not grant powers to authorities and do not prevent unauthorised covert activity taking place. However, unauthorised activity may result in a claim for breach of human rights against the County Council, and in cases where the covert activity has secured evidence for use in criminal trials, that evidence may be excluded by a judge as unfairly obtained.

2.2 The trading standards service uses RIPA and IPA in the course of investigations into offences contrary to consumer protection legislation and the Fraud Act 2006, and conspiracy to defraud contrary to common law. Veritau Ltd investigates theft from and fraud against the County Council and might also adopt covert techniques to secure evidence in such cases. Service departments will also investigate gross misconduct involving financial or other abuse of clients.

3.0 Covert Activity Policy

3.1 Executive Members and the Corporate Director (Business and Environmental Services) last reviewed the Covert Activity Policy on 26th October 2018. In November 2018 and June 2019, the changes to the process for the acquisition of communications data introduced by IPA came into force for local authorities. The policy, which is produced as appendix 1 to this report, has been updated to reflect the provisions of the new legislation. Revisions are marked in red.

3.2 Previously, RIPA set out three categories of communications data: traffic data, service use data and subscriber data. Local authorities were only permitted to acquire service use and subscriber data. The new Act replaces the three with two new categories: entity data and events data. Both categories are available to local authorities. However, local authorities are not permitted to acquire one type of events data, that being internet communication records. Both entity data and events data may only be acquired for the prevention or detection of crime, and in addition to obtain events data, the crime must be punishable by a maximum prison sentence of at least 12 months.

3.3 The Act requires local authorities to have a collaboration agreement with a body certified by the Secretary of State to act as the single point of contact with telecommunications providers. NYCC is a member of the National Anti-Fraud Network (NAFN) which is so certified. NYCC officers submit applications via the NAFN website. NAFN handles all contact with communications providers and also sends applications on to OCDA (see 3.4 below).

3.4 The Act introduced a central approval process for applications to acquire communications data. This removes the requirements for an NYCC senior officer to approve applications and for judicial approval (from the magistrates' court) to be sought for authorisations. The new central body is known as the Office for Communications Data Authorisations (OCDA) and is operated under the auspices of the Investigatory Powers Commissioner. A senior officer at NYCC must be 'aware' of the application before it is submitted to NAFN but no longer authorises or approves it.

4.0 Report on Covert Activity

4.1 From October 2018 to September 2019, authorisations under RIPA were granted for the following activities:

Date	Type of Authorisation	Investigation	Outcome
March 2019	Directed Surveillance	Fake jewellery	Home Office simple caution
March 2019	Covert Human Intelligence Source (CHIS)	Fake jewellery	Home Office simple caution

4.2 From October 2018 to September 2019, applications were made via NAFN and authorisations granted to acquire the following communications data:

Date	Type of Authorisation	Investigation	Outcome
March 2019	Subscriber data	Mis-described building work	Prosecution – sentence pending
May 2019	Subscriber data	Food safety	Investigation on-going
June 2019	Entity data	Mis-described building work	No further action
June 2019	Entity data x 3	Mis-described roofing work	On-going prosecution for conspiracy to defraud

Date	Type of Authorisation	Investigation	Outcome
June 2019	Event data x 3	Mis-described roofing work	On-going prosecution for conspiracy to defraud
July 2019	Entity data x 3	Mis-described product and aggressive practices	On-going investigation
August 2019	Entity data x 2	Mis-described roofing work	On-going prosecution for conspiracy to defraud
September 2019	Entity data	Counterfeit products	On-going investigation
October 2019	Entity data	Counterfeit products	On-going investigation

5.0 Training

5.1 It is a requirement of the policy that annual training is undertaken by relevant staff. The RIPA co-ordinator attended a seminar provided by NAFN, and at which IPCO presented, on 21 November 2019 and 30 staff from trading standards and legal and democratic services are undertaking a training session from an external provider on 29 November 2019.

6.0 Oversight

6.1 In October 2018, the newly formed Investigatory Powers Commissioner's Office (IPCO) undertook a remote inspection. This involved a review of the policy and previous applications and had a positive outcome. The policy was described as well written and easy to read, and it was noted that there was a good level of corporate and political engagement.

6.2 Oversight of communications data requests takes the form of an IPCO inspection at the NAFN offices. NAFN has also recently had a successful audit.

7.0 Legal Implications

7.1 Reviewing and reporting on the policy and its use enable compliance with the Acts and codes of practice issued under RIPA. There are no other legal implications from this report itself although ensuring that a policy is in place and properly implemented helps to protect the County Council from claims for breaches of article 8 of the European Convention on Human Rights (the right to a private and family life) and from the exclusion of evidence in criminal proceedings.

8.0 Financial Implications

8.1 There are no financial implications arising from this report.

9.0 Equalities Implications

9.1 A decision record sheet covering the decision not to complete an equalities impact assessment has been submitted and signed off.

10.0 Recommendations

10.1 That BES Executive Members and the Corporate Director (BES) note the use made of RIPA from October 2018 – September 2019.

10.2 That BES Executive Members and the Corporate Director (BES) approve the revised Covert Activity Policy.

Matt O'Neill
Assistant Director - Growth, Planning and Trading Standards

Author of report: Jo Boutflower, Head of Business and Consumer Services

Background documents: None

COVERT ACTIVITY POLICY

SCOPE:
This policy applies to all employees of North Yorkshire County Council.

PURPOSE:
- To set the criteria under which authorisation of covert activity under the Regulation of Investigatory Powers Act 2000 may be granted.
- To set the criteria under which authorisation of covert activity outside the Regulation of Investigatory Powers Act 2000 may be granted.
- To designate officers who may authorise covert activity.
- To set requirements for the internal oversight of covert activity.

1. THE LEGAL FRAMEWORK

The European Convention on Human Rights (ECHR) was incorporated into UK law by the Human Rights Act 1998. Article 8 of ECHR sets out that everyone has the right to *"…respect for his private and family life, his home and his correspondence",* and that a local authority may not interfere with this right except "…*as is in accordance with the law and is necessary in a democratic society… for the prevention of…crime…*"[1]

The Regulation of Investigatory Powers Act 2000 (RIPA) was enacted to put a framework in place to allow for the lawful interference of an individual's article 8 rights in compliance with ECHR. It was supplemented by the Investigatory Powers Act 2016 (IPA) and the Acts defines three types of covert activity which may be undertaken by local authorities. These are:

1.1 Directed Surveillance

This is surveillance which is not intrusive[2] but which is targeted at an individual or individuals, is covert, and is likely to result in the obtaining of private information[3].

Private information includes any information relating to a person's private or family life[4], including family or professional/business relationships. Information which appears public, such as conversations in the street or material posted on social media, may still be private information as it will be likely that the individual has a reasonable expectation of privacy even though they are acting in public[5].

1.2 Covert Human Intelligence Sources (CHIS)

A person is a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:
- the covert use of such a relationship to obtain information or to provide access to any information to another person; or
- the covert disclosure of information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.[6]

---

[1] RIPA sets out other statutory grounds (ss. 22(2), 28(3) and 29(3)) but local authorities may only use RIPA 'for the preventing or detecting of crime' (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and Regulation of Investigatory Powers (Communications Data) Order 2010. See also s. 60A(7) Investigatory Powers Act 2016 IPA

[2] Intrusive surveillance is surveillance that takes place on residential premises or in a private vehicle by means of an individual or surveillance device on the premises or in the vehicle (S.26(3) RIPA).

[3] S.26(2) RIPA

[4] S.26(10) RIPA

[5] Para 3.4, page 16, Covert Surveillance and Property Interference Code of Practice (August 2018)

[6] S.26(8) RIPA

1.3 Acquisition of Communications Data

Communications data is the 'who', 'when', 'where' and 'how' of a communication but not the content. There are currently 2 categories of communications data:

Entity data[7] - which identifies the location a communication was sent from or its destination. It includes IP addresses, cell site (location by triangulation from mobile phone masts) data, online parcel tracking.

Events data[8] - the use made by a person of a communication service. This would include outgoing call logs or information about redirection services.

Local authorities may not obtain internet connection records, a type of events data.

1.4 Restricted Covert Activity

Local authorities may not undertake the following types of covert activity under the framework:

- Intrusive surveillance[9],
- Property interference[10], or
- The interception of communications[11].

Intrusive surveillance is surveillance that takes place on residential premises or in a private vehicle by means of an individual or surveillance device on the premises or in the vehicle. Property interference is the entry onto or interference with property or wireless telegraphy. It would include, for example, the fitting of a tracking device to a vehicle[12] or the installation of a recording device in a residential property. The interception of a communication is anything which obtains the content of that communication, for example, placing a wiretap on a phone.

1.5 Authorisation of Covert Activity under RIPA

Covert activity which meets the RIPA criteria must be authorised in accordance with the Act. An application must be made on the appropriate form[13] and authorised by an officer meeting the prescribed offices, ranks, and position[14]. The authorisation will not be valid until judicial approval has been obtained from a magistrates' court[15] and so covert activity must not take place until both the internal authorisation and judicial approval have been obtained. Authorisations must be cancelled as soon as the activity is concluded[16]. Further information about the authorisation process can be found in the Covert Activity Procedures document.

1.6 Authorisation of Covert Activity outside RIPA

The Investigatory Powers Tribunal has considered the authorisation and use of covert activity outside the RIPA framework. It has observed that:

---

[7] S.261(3) of the Investigatory Powers Act 2016 (IPA)

[8] S.261 (4) IPA – see also s. 62 IPA for the restriction in relation to internet connection records

[9] S.26(3) RIPA

[10] Paragraph 7.1, page 56, Covert Surveillance and Property Interference Code of Practice (August 2018)

[11] Ss.18 and 73 IPA

[12] It is not property interference for a vehicle owner or operator to fit such a device, see paragraph 7.49, page 66, Covert Surveillance and Property Interference Code of Practice (August 2018) for public authority vehicles

[13] Current forms may be obtained from the trading standards service, legal services or Veritau

[14] The list of current authorising officers & designated officers can be found at Annex 1

[15] Ss. 37 & 38 Protection of Freedoms Act 2012

[16] Regulation of Investigatory Powers (Cancellation of Authorisation) Regulations 2000

"RIPA does not require prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation does not necessarily mean that the carrying out of directed surveillance is unlawful"[17].

The tribunal has considered in detail the process of authorising activity outside RIPA. The case[18] involved the placing of a covert silent video recorder in the sitting room of a flat occupied by a severely disable young woman in response to a number of petty thefts. The thefts did not meet the 'serious'[19] threshold for intrusive surveillance under RIPA. A superintendent had authorised the covert activity and had recorded her reasons:

"…the particular conduct could not be authorised under RIPA but that this did not necessarily mean that the actions proposed could not be lawfully undertaken, even though it would be without the protection that an authorisation under RIPA would afford. The Act itself states that any such deployment outside RIPA does not necessarily mean that it is unlawful."[20]

The superintendent had considered the necessity and proportionality of the activity and the risk of collateral intrusion. She had also considered guidance issued by the Office of the Surveillance Commissioner.[21]

The Investigatory Powers Tribunal agreed with the submission by Cleveland Police that the force had acted "…exactly as the public would have expected it to act". The tribunal endorsed the procedure adopted by the superintendent, "i.e. a procedure as close as possible to that which would be adopted if an authorisation could be obtained from a…relevant authorising officer [under RIPA]."

1.7 Authorisation of the Acquisition of Communications Data

Communications data may only be obtained using the IPA framework. Other statutory powers must not be used to acquire communications data.

Applications must be made via a collaboration agreement partner, currently NAFN, and approved by the Office for Communications Data Authorisations. Applicants must make a relevant senior officers (as listed in Annex 1) aware of the application before it is submitted.

All contact with a communications provider must be via the single point of contact (SPOC) employed by the collaboration partner.

2. USE OF COVERT ACTIVITY BY NYCC OFFICERS

Covert techniques may be used by NYCC officers acting in the course of their employment only in the accordance with the table set out in Annex 2 of this policy. Where a company or individual[22] is contracted by NYCC to undertake covert activity, such activity must be authorised as if it was undertaken by NYCC employees and only in accordance with the table in Annex 2.

---

[17] C and the Police & Secretary of State for the Home Department IPT/03/32/H
[18] BA & others and the Chief Constable of Cleveland Police IPT/11/129/CH, IPT/11/133/CH & IPT/12/72/CH
[19] Intrusive surveillance may only be undertaken in relation to 'serious' crime as defined by ss.80(2) &(3)
[20] S.80 (general saving for lawful conduct)
[21] OSC Procedures & Guidance, December 2011, paragraphs 231-233
[22] Including Veritau Ltd when acting as NYCC's internal fraud investigator

Authorised covert activity may only be undertaken in accordance with the Covert Activity Procedures. This document is maintained by the RIPA Co-ordinating Officer, from whom a copy can be obtained.

The welfare obligations arising from the use and conduct of CHIS are such that NYCC is not equipped to meet them properly. Accordingly, third party (non-employee) CHIS will only be deployed in joint operations with a police force in situations where the force concerned can source, authorise, manage and safeguard the CHIS.

Surveillance product must be stored and disposed of in accordance with the Documents and Records Management Policy, and only used for the purpose for which it was obtained.

If covert activity concerns the acquisition of communications data, the National Anti-Fraud Network (NAFN)[23] must be used to fulfill the SPOC function.

3. SENIOR RESPONSIBLE OFFICER

The senior responsible officer is the Assistant Director (Growth, Planning and Trading Standards) reporting to the Corporate Director (Business and Environmental Services). He is responsible for[24]:

- ensuring authorising officers are of an appropriate standard,
- ensuring the integrity of the CHIS process,
- overseeing the reporting of errors,
- implementing any action plans following inspections.

4. RIPA CO-ORDINATOR

The RIPA co-ordinator function is provided by the trading standards service[25]. The RIPA co-ordinator undertakes the following functions:

- maintains a central record or directed surveillance and CHIS[26],
- contacts the nominated officer in each relevant service area to obtain quarterly updates on training needs,
- manages the arrangement and provision of appropriate training,
- maintains the Covert Activity Policy and Covert Activity Procedures documents.

5. TRAINING

Any officer who intends to apply for a covert activity authorisation must receive appropriate training and all officers using covert techniques will receive on-going annual training relevant to their covert activities and responsibilities. This must be considered as part of the annual appraisal process for relevant employees. The RIPA co-ordinator maintains a register of training needs.

---

[23] See Annex 1 for contact details to obtain access to NAFN. A collaboration agreement is now a requirement by virtue of s. 74 IPA

[24] Paragraph 4.41, page 39 Covert Surveillance and Property Interference Code of Practice (August 2018) and paragraph 9.1, page 55, Covert Human Intelligence Sources Code of Practice (August 2018)

[25] See Annex 1 for contact details

[26] Paragraphs 8.1 and 8.2, pages 68-69, Covert Surveillance and Property Interference Code of Practice (August 2018) and paragraph 7.1, page 35, Covert Human Intelligence Sources Code of Practice (August 2018)

6. **OVERSIGHT**

BES Executive Members receive quarterly updates on the use of RIPA, and also consider an annual report on the Covert Activity Policy to ensure that it is fit for purpose and being implemented properly.

ANNEX1

Authorising Officers
Head of Paid Service
Chief Executive

Legal & Democratic Services
Assistant Chief Executive (Legal & Democratic Services) (Acting Head of Paid Service in the absence of the Chief Executive)
Legal Manager (People)
Legal Manager (Corporate Services)

Growth, Planning and Trading Standards
Head of Business & Consumer Services
Head of Multi-agency Safeguarding Team

Senior Responsible Officer
Assistant Director (Growth, Planning and Trading Standards)

RIPA Coordinating Officer
Head of Business and Consumer Services – in respect of training and day to day management
Intelligence and Information Assets Officer – in respect of the central record, source record and audit

To arrange authorisation to access NAFN please contact the Head of Business and Consumer Services

ANNEX 2

Covert activity may only be undertaken in accordance with this table:

ACTIVITY[27]	SERVICE[28]	PURPOSE
DS	TS	investigations into criminal offences suspected to have been committed in connection with the supply of goods or services by a business to consumer(s) and which attract at least a maximum penalty of up to six months' imprisonment
DS	TS	investigations into suspected criminal offences arising from the sale of alcohol or tobacco products to those under the age of 18
DS	IF	investigations into theft and fraud perpetrated against NYCC
NR-IS	TS	investigations into fraud and unfair commercial practices[29] perpetrated in a repeated and targeted manner against vulnerable residents
NR-IS	IF	investigations into fraud or theft perpetrated against a resident of County Council residential premises.
NR-IS	IF or service depts	Investigations into gross misconduct by an NYCC employee involving financial or other abuse of NYCC clients.
CHIS	TS	to facilitate online test purchase operations involving the use of a covert identity and communication with an individual suspected of a criminal offence suspected to have been committed in connection with the supply of goods or services by a business to consumer(s) and which attracts at least a maximum penalty of up to six months' imprisonment
CHIS	TS	to facilitate face to face test purchase operations and/or to collect goods ordered online from an individual suspected of a criminal offence suspected to have been committed in connection with the supply of goods or services by a business to consumer(s) and which attracts at least a maximum penalty of up to six months' imprisonment
CD	TS	Events and/or entity data for investigations into criminal offences suspected to have been committed in connection with the supply of goods or services by a business to consumer(s)
CD	IF	investigations into theft and fraud perpetrated against NYCC

[27] DS = directed surveillance, CHIS = use and conduct of a covert human intelligence source, CD = acquisition of communications data, NR-DS = directed surveillance outside RIPA, NR-IS = intrusive surveillance authorised outside RIPA

[28] TS = trading standards, IF = internal fraud investigators (Veritau Ltd)

[29] As defined by the Consumer Protection from Unfair Trading Regulations 2008