

**North Yorkshire County Council**

**Business and Environmental Services**

**Executive Members**

**18 December 2020**

**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 BES Executive Members and the Corporate Director (BES) 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 2019 to September 2020.

**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 does 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 11 December 2019. In August 2020 the Investigatory Powers Commissioner wrote to all public authorities to remind them of their data safeguarding responsibilities in respect of material generated by covert activity. Authorising officers already include instructions on the retention and disposal of such material within their written authorisations to applicants. However, proposed amendments have been incorporated into the policy at paragraph 1.8 to reference the chapters on data safeguarding in the respective statutory codes of practice and to make it clear that the corporate Document Management and Records Retention Policy must be followed. The amendments are marked in red on the policy, which is produced at Appendix A.

3.2 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 for the acquisition of communications data under IPA. NYCC continues to be a member of the National Anti-Fraud Network (NAFN), which is so certified. NYCC officers make applications via the NAFN website. NAFN completes all contact with communications providers, and submits applications on to the Office for Communications Data Authorisations (OCDA).

#### 4.0 Report on Covert Activity

4.1 From October 2019 to September 2020, there were no applications or authorisations for directed surveillance or use of a covert human intelligence source (CHIS) under RIPA.

4.2 From October 2019 to September 2020 applications were made via NAFN, and authorisations granted to acquire the following communications data:

Date	Type of Authorisation	Investigation	Outcome
October 2019	Entity data x 3	Illicit tobacco	Informal caution
December 2019	Entity data Event data (3 numbers)	Roofing work	Fraud prosecution on-going
January 2020	Entity data	Illicit tobacco	Informal caution
February 2020	Entity data Event data (3 numbers)	Home improvement work	On-going prosecution for conspiracy to defraud
May 2020	Entity data	Home improvement work	On-going prosecution for conspiracy to defraud
June 2020	Entity data Event data (3 numbers)	Mis-described home improvement work	On-going investigation
August 2020	Entity data Event data (3 numbers)	Mis-described home improvement work	On-going investigation
September 2020	Entity data Event data (4 numbers)	Home improvement work	On-going prosecution for conspiracy to defraud

#### 5.0 Training

5.1 The annual NAFN conference was planned to take place in York on 17 November 2020, and would have provided training for staff. The conference did not take place as a consequence of covid restrictions. NAFN has developed an online learning platform and has received Home Office funding to provide investigatory powers training to enforcement officers. This training should be available early in the new year and will be rolled out to all staff undertaking work involving covert activity.

## **6.0 Oversight**

- 6.1 The Investigatory Powers Commissioner's Office (IPCO) undertakes periodic inspections of the Authority. No inspection took place during the reporting period.
- 6.2 IPCO requires an annual return of the numbers of directed surveillance and CHIS authorisations granted for the calendar year by 31 January in the following year. Figures for 2019 were returned to IPCO on 22 January 2020. The next return is due by 31 January 2021.
- 6.3 Oversight of communications data requests takes the form of an annual IPCO inspection at the NAFN offices. NAFN was audited in October 2020 and received a good report with no recommendations or action points.

## **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. Appendix B.

## **10.0 Recommendations**

- 10.1 That BES Executive Members and the Corporate Director (BES) note the use made of RIPA from October 2019 – September 2020.
- 10.2 That BES Executive Members and the Corporate Director (BES) approve the continued use of the Covert Activity Policy.

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

Author of report: Jo Bouflower, 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...*”<sup>1</sup>

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<sup>2</sup> but which is targeted at an individual or individuals, is covert, and is likely to result in the obtaining of private information<sup>3</sup>.

Private information includes any information relating to a person’s private or family life<sup>4</sup>, 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<sup>5</sup>.

#### 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.<sup>6</sup>

---

<sup>1</sup> 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

<sup>2</sup> 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).

<sup>3</sup> S.26(2) RIPA

<sup>4</sup> S.26(10) RIPA

<sup>5</sup> Para 3.4, page 16, Covert Surveillance and Property Interference Code of Practice (August 2018)

<sup>6</sup> 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**<sup>7</sup> - 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**<sup>8</sup> - 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<sup>9</sup>,
- property interference<sup>10</sup>, or
- the interception of communications<sup>11</sup>.

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<sup>12</sup> 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<sup>13</sup> and authorised by an officer meeting the prescribed offices, ranks, and position<sup>14</sup>. The authorisation will not be valid until judicial approval has been obtained from a magistrates’ court<sup>15</sup> 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<sup>16</sup>. Further information about the authorisation process can be found in the Covert Activity Procedures document.

---

<sup>7</sup> S.261(3) of the Investigatory Powers Act 2016 (IPA)

<sup>8</sup> S.261 (4) IPA – see also s. 62 IPA for the restriction in relation to internet connection records

<sup>9</sup> S.26(3) RIPA

<sup>10</sup> Paragraph 7.1, page 56, Covert Surveillance and Property Interference Code of Practice (August 2018)

<sup>11</sup> Ss.18 and 73 IPA

<sup>12</sup> 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

<sup>13</sup> Current forms may be obtained from the trading standards service, legal services or Veritau

<sup>14</sup> The list of current authorising officers & designated officers can be found at appendix 1

<sup>15</sup> Ss. 37 & 38 Protection of Freedoms Act 2012

<sup>16</sup> Regulation of Investigatory Powers (Cancellation of Authorisation) Regulations 2000

## 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:

*“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”<sup>17</sup>.*

The tribunal has considered in detail the process of authorising activity outside RIPA. The case<sup>18</sup> involved the placing of a covert silent video recorder in the sitting room of a flat occupied by a severely disabled young woman in response to a number of petty thefts. The thefts did not meet the ‘serious’<sup>19</sup> 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.”<sup>20</sup>*

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.<sup>21</sup>

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 officer (as listed in appendix 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.

<sup>17</sup> C and the Police & Secretary of State for the Home Department IPT/03/32/H

<sup>18</sup> BA & others and the Chief Constable of Cleveland Police IPT/11/129/CH, IPT/11/133/CH & IPT/12/72/CH

<sup>19</sup> Intrusive surveillance may only be undertaken in relation to ‘serious’ crime as defined by ss.80(2) &(3)

<sup>20</sup> S.80 (general saving for lawful conduct)

<sup>21</sup> OSC Procedures & Guidance, December 2011, paragraphs 231-233

## 1.8 Data Assurance

Regard must be had to the guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained by the use of covert means set out in each code of practice<sup>22</sup>.

Such material must be clearly labelled and identified on each data pathway on which it is stored. Applications should identify the data pathways to be used to store material in order that the authorising officer understands where it will be stored and can give appropriate instructions within the authorisation. Officers must comply with the North Yorkshire County Council Documents and Record Management Policy and covert activity procedures in allocating a retention period to material.

The annual report to Members includes the results of data safeguarding dip sampling which is undertaken by the RIPA co-ordinator.

## 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 appendix 2 of this policy. Where a company or individual<sup>23</sup> 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 appendix 2.

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)<sup>24</sup> must be used to fulfill the SPOC function.

---

<sup>22</sup> Chapter 9, Covert Sureveillance and Property Interference Revised Code of Practice, August 2018

Chapter 8, Covert Human Intelligence Sources Revised Code of Practice, August 2018

Chapter 7, Acquisition and Disclosure of Communications Data Code of Practice, March 2015

<sup>23</sup> Including Veritau Ltd when acting as NYCC's internal fraud investigator

<sup>24</sup> See appendix 1 for contact details to obtain access to NAFN. A collaboration agreement is now a requirement by virtue of s. 74 IPA

### 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<sup>25</sup>:

- 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<sup>26</sup>. The RIPA co-ordinator undertakes the following functions:

- maintains a central record or directed surveillance and CHIS<sup>27</sup>,
- 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.

### 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.

---

<sup>25</sup> 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)

<sup>26</sup> See appendix 1 for contact details

<sup>27</sup> 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)



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

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

<b>ACTIVITY<sup>28</sup></b>	<b>SERVICE<sup>29</sup></b>	<b>PURPOSE</b>
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 <sup>30</sup> 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

<sup>28</sup> 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

<sup>29</sup> TS = trading standards, IF = internal fraud investigators (Veritau Ltd)

<sup>30</sup> As defined by the Consumer Protection from Unfair Trading Regulations 2008

<b>Initial equality impact assessment screening form</b> (As of October 2015 this form replaces 'Record of decision not to carry out an EIA')			
<b>This form records an equality screening process to determine the relevance of equality to a proposal, and a decision whether or not a full EIA would be appropriate or proportionate.</b>			
<b>Directorate</b>	BES		
<b>Service area</b>	Trading Standards		
<b>Proposal being screened</b>	Revised Covert Activity Policy		
<b>Officer(s) carrying out screening</b>	Jo Boutflower		
<b>What are you proposing to do?</b>	Review and amend the covert activity policy to include details of data assurance methods.		
<b>Why are you proposing this? What are the desired outcomes?</b>	To ensure that covert activity and the acquisition of communications data can be undertaken in appropriate circumstances in a lawful, necessary and proportionate manner with safeguards in place to protect the human rights of third parties, and clients and employees of the County Council.		
<b>Does the proposal involve a significant commitment or removal of resources? Please give details.</b>	No.		
<b>Is there likely to be an adverse impact on people with any of the following protected characteristics as defined by the Equality Act 2010, or NYCC's additional agreed characteristics?</b> As part of this assessment, please consider the following questions: <ul style="list-style-type: none"> <li>To what extent is this service used by particular groups of people with protected characteristics?</li> <li>Does the proposal relate to functions that previous consultation has identified as important?</li> <li>Do different groups have different needs or experiences in the area the proposal relates to?</li> </ul> <b>If for any characteristic it is considered that there is likely to be a significant adverse impact or you have ticked 'Don't know/no info available', then a full EIA should be carried out where this is proportionate. You are advised to speak to your <a href="#">Equality rep</a> for advice if you are in any doubt.</b>			
<b>Protected characteristic</b>	<b>Yes</b>	<b>No</b>	<b>Don't know/No info available</b>
Age		X	
Disability		X	
Sex (Gender)		X	
Race		X	
Sexual orientation		X	
Gender reassignment		X	
Religion or belief		X	
Pregnancy or maternity		X	
Marriage or civil partnership		X	
<b>NYCC additional characteristic</b>			
People in rural areas		X	

People on a low income		X	
Carer (unpaid family or friend)		X	
<b>Does the proposal relate to an area where there are known inequalities/probable impacts</b> (e.g. disabled people's access to public transport)? Please give details.	No.		
<b>Will the proposal have a significant effect on how other organisations operate?</b> (e.g. partners, funding criteria, etc.). <b>Do any of these organisations support people with protected characteristics?</b> Please explain why you have reached this conclusion.	No.		
<b>Decision (Please tick one option)</b>	EIA not relevant or proportionate:	X	Continue to full EIA:
<b>Reason for decision</b>	<p>The amended policy ensures that covert activity is only undertaken where the impact, and particularly the right to respect for private and family life under article 8 of the European Convention on Human Rights, on anyone who is the subject of, or collateral to, the covert activity has been considered and that it is considered by a senior officer that despite the risk of intrusion, the activity is necessary and proportionate bearing in mind the objective it seeks to achieve, and that the policy reflects the current law.</p> <p>The revised policy will ensure that covert activity is deployed in a consistent manner and that it is not deployed in response to an individual's protected characteristics.</p>		
<b>Signed (Assistant Director or equivalent)</b>	Matt O'Neill		
<b>Date</b>	23/11/20		