Hambleton District Council

Report To:	Audit, Governance and Standards Committee
Date:	20 October 2020
From:	Director of Law and Governance (Monitoring Officer)
Subject:	**Regulation of Investigatory Powers Act 2000 – Inspection by the Investigatory Powers Commissioner's Office**
Portfolio Holder:	Governance Councillor Mrs I Sanderson
Wards Affected:	All Wards

1.0 Purpose and Background:

1.1 To report to the Committee the findings of the Investigatory Powers Commissioner following his recent inspection and to ask the Committee to endorse the actions taken to implement the Commissioner's recommendations.

1.2 To receive the latest reports on any activities which have been authorised under the Regulation of Investigatory Powers Act 2000 ("RIPA").

2.0 Inspection by the Investigatory Powers Commissioner's Office

2.1 The Investigatory Powers Commissioner carried out his three-yearly inspection on 20th August 2020. A copy of the Commissioner's inspection report is attached at "Appendix A". The report was generally positive, but suggested the following actions:-

2.1.1 minor revisions to the Council's RIPA Guide to Practice and Procedure, namely to enhance the section dealing with officers using social media in their official capacity, and to further embed the data security safeguards relating to the use of covert powers;

2.1.2 minor amendments to the Central Register of Authorisations, namely to include an additional entry dealing with the destruction of any covert surveillance material;

2.1.3 to revise the Council's corporate Information Management Policy and Information Asset Register to highlight the safeguards for dealing with RIPA information, namely by referring people to the RIPA Guide to Practice and Procedure which addresses these issues;

2.1.4 to consider reducing the reports to Committee on the use of RIPA powers from quarterly to six-monthly reports.

2.2 Attached at Appendices "B" and "C" respectively are the Council's updated RIPA Guide to Practice and Procedure and Central Register of Authorisations.

2.3 Paragraph 10.3 of the revised RIPA Guide emphasises the need to comply with the safeguarding obligations set out in the Home Office's relevant Codes of Practice. Paragraphs 21.5 and 21.6 of the Guide address the use of social media. The Information Management Policy and Information Asset Register are being revised in line with the recommendations.

2.4 The Central Register of Authorisations now contains additional entries dealing with the destruction of covert surveillance material and the officer responsible. The steps detailed in this report adequately address the recommendations of the Investigatory Powers Commissioner set out at paragraphs 2.1.1 – 2.1.3 above.

2.5 In line with the Commissioner's suggestion set out at paragraph 2.1.4 of this report it is proposed that the frequency of the RIPA activity reports is reduced from its current quarterly format to six-monthly reports. There have been no RIPA authorisations in recent years and suitable oversight by the Committee can still be achieved with bi-annual reports.

3.0 RIPA Activities

3.1 Although RIPA covers a number of activities undertaken by investigatory bodies (e.g., phone tapping by the Security Services and Police) its principle use in respect of Local Authorities relates to:-

- covert surveillance, and
- covert human intelligence sources.

3.2 Covert surveillance covers the monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained. RIPA is most relevant to the Council's activities in effecting enforcement procedures such as the investigation and prosecution of offences. This would not normally include the initial investigation of contraventions such as planning enforcement or noise investigations, but would normally involve the later stages where criminal activity was a possibility. Although this could technically include breaches of Planning Enforcement Notices, breaches of Environmental Health Notices, fraud, etc., the Council's use of the powers has been very limited in recent years. For example, the Council has not used authorisations under the Act in the last three years.

3.3 Since 1 November 2012 the Council has only been able to use RIPA for directed surveillance for potential criminal activity with a possible penalty of at least six months imprisonment. This means that the Council is unable to use the procedure for low-level offences such as littering or dog control. For serious offences the Council needs approval from a magistrate before it can use directed surveillance.

3.4 Another use of the Act is for the Police to authorise use of the Council's CCTV system for specific operations (general use of CCTV is not covered by the Act because this is not covert surveillance). The Police authorise themselves to use the Council's CCTV system for covert surveillance on approximately two occasions per year.

3.5 Covert human intelligence sources relate to the use of a third party to gather information. For example, this could be an informer or someone used to undertake test purchases. This is not an activity that the Council engages in at all. The Council also needs the approval of a magistrate to carry out this activity.

3.6 The only area in which the Council might very occasionally involve itself where RIPA might be relevant is covert surveillance. It is necessary for the Council therefore to follow the legislation and the requirements of Government Codes of Practice. Most of the requirements of the Code are dealt with at an Officer level. However, Members are expected to approve a Policy on RIPA and to have some involvement in the monitoring of how the Council implements RIPA requirements.

4.0 Monitoring of RIPA Activity

4.1 Codes of Practice on RIPA recommend that regular reports are made to Members on RIPA activity. Consideration of such reports has been delegated to the Audit, Governance and Standards Committee. This report therefore constitutes one of those reports and is intended to cover the period 22 January 2020 to 20 October 2020. There were no authorisations during this period. It is recommended that the Committee note the position.

5.0 Recommendations

5.1 It is recommended that:-

(1) the position in respect of the inspection by the Investigatory Powers Commissioner's Office is noted;

(2) the steps taken to comply with the Commissioner's findings are endorsed and the Council's updated RIPA Guide to Practice and Procedure Policy and Central Record of Authorisations are approved;

(3) it be noted that no RIPA authorisations were made by the Council during the period 22 January 2020 to 20 October 2020; and

(4) the frequency of the RIPA activity reports is reduced from quarterly reports to six-monthly reports.

Gary Nelson
Director of Law and Governance (Monitoring Officer)

Background papers: HDC RIPA Register of Authorisations
Author ref: GN
Contact: Gary Nelson
Director of Law and Governance (Monitoring Officer)
Direct Line No: (01609) 767012

IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Dr Justin Ives
Chief Executive
Hambleton District Council
Civic Centre
Stone Cross
Rotary Way
Northallerton
North Yorkshire
DL6 2UU

21 August 2020

Dear Dr Ives,

Remote Inspection of Hambleton District Council

Please be aware that IPCO is not a "public authority" for the purpose of the Freedom of Information Act (FOIA) and therefore falls outside the reach of the FOIA. It is appreciated that local authorities are subject to the FOIA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.

Due to the ongoing Coronavirus situation your authority was recently subject to a remote inspection by one of my Chief Inspectors, Mrs Clare Ringshaw-Dowle. All the documentation and arrangements necessary for my Chief Inspector to carry out the process was provided by Mr. Gary Nelson, your Director of Law and Governance, who also holds the position of RIPA Coordinator. Both you, as Senior Responsible Officer, and Mr Nelson made yourselves available to be interviewed via telephone by Mrs Ringshaw-Dowle, and from the documentation examined and the information provided during the interview, the level of compliance shown by your authority removes, for the present, the requirement for a physical inspection.

At the last inspection, conducted by the OSC in late 2016, your authority was subject to five recommendations, all of which can now be discharged.

Your RIPA Policy was provided in advance of the inspection and Mrs Ringshaw-Dowle has given you some suggestions for its next iteration. The main revisions are to enhance the section dealing with officers using social media in their official capacity, and to embed the Safeguards relating to use of covert powers as previously covered in my letter to you regarding Data Assurance. The Policy was otherwise in good shape and has been maintained in accordance with the Home Office Code of Practice requirement that it be endorsed by your Elected Members on an annual basis.

The Council has six designated Authorising Officers which provides a good level of resilience, but in the absence of use of the powers over the last decade, you might feel a reduced cadre would suffice.

I am pleased to learn that externally provided RIPA training has been maintained (last provided in 2016 by Act Now) and is being planned for later this year, following its postponement from June due to the pandemic. Ongoing refresher training has been provided in between times by Mr Nelson, with Directors, Heads of Service and Managers of those departments most likely to consider using the powers.

In terms of internal governance of covert powers, and despite their non-usage, Mr Nelson is clearly aware of the need to ensure RIPA, and now the Investigatory Powers Act 2016, is kept in the minds of all Council officers, not just those with an obvious enforcement or investigative role. To do what he can to ensure that activities are not being conducted outwith the auspices of RIPA, Mr Nelson carefully scrutinises Council investigations and has discussions with managers and legal teams to ensure that where prosecutions or enforcement action is to be taken, that the evidence has been appropriately obtained.

Over and above these checks, it is a matter of Council policy that before any officer starts to put together an application for use of the powers, they first run the matter past Mr Nelson. In this way, he can offer initial advice on the suitability or not of using covert means, and is alive to any subsequent request to an Authorising Officer. The lack of usage was discussed, and is the result of various developments: the passage of most benefit fraud cases to the DWP; the use of alternative statutory powers for things like Planning and Environmental Health; the preference for an overt approach, such as interviews under caution; and also, it was felt, a slight reluctance by officers to use powers which have dropped off in terms of their experience.

The Council operates a fixed and mobile CCTV camera system, with an associated Policy which was provided to my Chief Inspector. The system is run in accordance with the associated Code of Practice and the advice of the Surveillance Camera Commissioner; and his Third Party Self Certification has been completed and similarly provided for inspection.

You have received my earlier letter regarding Data Assurance which has prompted internal discussion and my Chief Inspector was pleased to see that the retention, review and disposal policies in relation to both authorisation paperwork and also any product from surveillance activities, has already been captured to a good degree within your RIPA Policy, and Mr Nelson said that an application for directed surveillance or a CHIS will not be authorised absent a suitable written plan in relation to the management and subsequent review and disposal of any product.

It has been suggested that Mr Nelson ensures the next revision of your Policy document is in line with the Safeguards chapter of the 2018 Codes of Practice and that there will be a suitable audit trail for the eventual destruction of product, including the means by which an officer(s) will be designated to check this is being carried out as intended (an additional entry in the Central Record may be a suitable means to capture this). It was also suggested that your Information Management Policy and Information Asset Register (both provided for inspection) should both contain at least a mention of the Safeguards for RIPA/IPA product, perhaps with a link to the main RIPA Policy section for further advice. The CCTV Policy already picks up the pathways for recorded material from that system, and similarly robust practices for any product from conventional surveillance or use of a CHIS might helpfully echo the clear advice and processes already in active use for CCTV.

You provide quarterly reports on the non-use of powers to your Elected Members via the Audit Governance and Standards Committee as well as the annual RIPA Policy endorsement, and Mrs Ringshaw-Dowle suggested you could reduce to a six-monthly interim update if that situation continues; but this is a matter for you and your Members to determine.

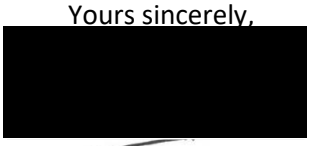
Your Council is registered with the National Anti Fraud Network (NAFN) and there was a brief outline provided of its role and the range of data that can be obtained through its services, which have not yet been used.

In conclusion, whilst there has been no use of these powers for many years, your Council has the requisite policies, training and internal governance arrangements in place and overseen by an experienced RIPA Coordinator, to suggest that where they are used in future, the levels of compliance should be of a good standard.

I hope that you find the outcome of this remote inspection helpful and constructive, and my Office is available to you should you have any queries following the receipt of this letter, or at any point in the future. I should be grateful if you can acknowledge the findings within the next two months.

The Chief Inspector would like to thank you and Mr. Nelson for your personal engagement and providing the necessary documentation to enable this remote inspection. Your time afforded during the current pandemic is much appreciated by IPCO.

Yours sincerely,



The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

Appendix B

HAMBLETON
DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDE TO PRACTICE AND PROCEDURE UNDER THE ACT

HAMBLETON DISTRICT COUNCIL

Date: August 2020
Review date: March 2021

THE REGULATION OF INVESTIGATORY POWERS AT 2000

GUIDE TO PRACTICE AND PROCEDURE UNDER THE ACT

PRACTICE

1. Introduction

1.1 The main purpose of the Regulation of Investigatory Powers Act 2000 ("the Act") is to ensure that public bodies use their investigatory powers in accordance with the Human Rights Act 1998. The investigatory powers covered by the legislation are:-

(a) intrusive surveillance (on resident premises/in private vehicles) (NB: The Council is not permitted to engage in intrusive surveillance);

(b) covert surveillance in the course of specific operations;

(c) the use of covert human intelligence sources (agents, informants, undercover officers);

1.2 For each of these powers the Act ensures that the law clearly covers the purposes for which they may be used, which authorities can use the powers, who should authorise each use of power, the use that can be made of the material gained, independent judicial oversight and a means of redress for any individual aggrieved by use of the powers.

1.3 In addition to the legislation itself, the Home Office has issued Codes of Practice dealing with covert surveillance and covert human intelligence sources. This guide is designed to cover the aspects of RIPA that regulate the use of investigatory powers by the Council and should be read in conjunction with the Council's Policy Statement and the relevant Codes of Practice (see Appendix 2).

1.4 Directed Surveillance can only be undertaken if it is for the purpose of preventing/detecting a criminal offence which is punishable (whether on summary conviction or on indictment) by a maximum term of **at least 6 months of imprisonment** – or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (sale of tobacco and alcohol to underage children).

2. What is not regulated by RIPA?

2.1 Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. Thus, a local authority officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of his duties.

2.2 Surveillance which is not within the meaning of the legislation.

2.3 Overt CCTV surveillance systems are not normally covered by the Act as their use is obvious to the public. There may, however, be occasions where public authorities use material obtained from overt CCTV systems for the purposes of a specific investigation or operation, in such cases authorisation for direct surveillance may be necessary.

2.4 The Investigatory Powers Act 2016 regulates investigatory actions in respect of the acquisition of communications data. This is therefore outside the scope of this guide.

3. What is regulated by RIPA

3.1 The monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications where this is done in a manner calculated to ensure that the subject of surveillance is unaware that they are being monitored or observed etc.

3.2 The recording of anything monitored, observed or listened to during surveillance.

3.3 Use of a surveillance device, eg a hidden video camera, a listening device.

4. Rules of Evidence

4.1 Material obtained through covert surveillance may be used as evidence in criminal proceedings. Provided that surveillance has been properly authorised, the evidence gathered should be admissible under law and in accordance with Section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Material gathered as a result of surveillance authorised under the Act is subject to the ordinary rules for retention and disclosure of material and the Criminal Procedure and Investigations Act 1996.

5. Some Definitions

5.1	"Covert"	Concealed, done secretly
5.2	"Covert surveillance"	Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place
5.3	"Directed surveillance"	Surveillance which is covert, but not intrusive, and is undertaken for the purposes of a specific investigation or specific operation, in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) and otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the Act to be sought for the carrying out of the surveillance.
5.4	"Intrusive surveillance"	Covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

5.5 "Private Information" Includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

5.6 "Confidential Information: Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material.

6. Entering onto or interfering with property, or with wireless telegraphy or postal communications

6.1 Only members of the intelligence services are able to make applications to enter onto or interfere with property or with wireless telegraphy. Council staff are not permitted, under any circumstances, to engage in such activity.

6.2 It is an offence to intercept communications sent by public postal service and public telecommunication systems. Interception of communication can be done with lawful authority, however only a limited group can grant a warrant for such an activity (Secretary of State or his representative to such persons as the Directors-General of the Security Service and Director of GCHQ, the Chief of Secret Intelligence Service and the Chief Constables of Police). Therefore, it is not envisaged that the Local Authority would ever be permitted to make a lawful interception of a communication.

7. Authorisations

7.1 Purpose of Authorising Surveillance

7.1.1 An authorisation under the Act, with subsequent appropriate approval by a Justice of the Peace, provides lawful authority for a public authority to carry out surveillance. Responsibility for authorising surveillance investigations is given by an "authorising officer". Approval is then required by a Justice of the Peace. Surveillance must not be carried out without prior authorisation and approval (but see 2.1 above).

7.1.2 The consequence of not obtaining an authorisation and approval under the Act may be that the action is in breach of the Human Rights Act such that any evidence so gained could be excluded in any proceedings that arise.

7.1.3 The Home Office strongly recommends public authorities to seek an authorisation for surveillance that is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation.

7.2 Basis for Authorising Surveillance Activities

7.2.1 Authorisation can only be granted where there is justifiable interference with an individual's human rights, i.e. it is necessary and proportionate for surveillance activities to take place.

7.2.2 The authorising officer must believe that the authorisation is necessary in the circumstances of the particular case for the statutory grounds for directed surveillance to exist (see paragraph 12.1).

7.2.3 The authorising officer must also believe that the activity is proportionate to what is sought to be achieved. They must balance the intrusiveness of the activity proposed on both the target and others who may be affected, against the need for the activity in operational terms.

7.2.4 Before authorising surveillance the authorising officer must also take into account the risk of intrusion into the privacy of persons other than those who are the target of the investigation. This is known as collateral intrusion. The authorisation procedures allow for an assessment of collateral intrusion which the authorising officer will be required to consider prior to granting authorisation. In order to decide whether to grant authorisation the authorising officer must have a full picture of the operation, the proposed method(s) of observation and the Human Rights Act implications of the operation.

7.2.5 Where one agency acts on behalf of another, for example, this authority acts on behalf of a neighbouring authority, it is usually the responsibility of the tasking authority to obtain the authorisation. When staff are operating on another organisation's authority they must ensure that they have seen and understood the extent of the authorised activities. The will ensure staff act in accordance with the authorisation. A copy of the authorisation should also be taken and passed to the RIPA Co-ordinating Officer – who is the Director of Law and Governance.

7.2.6 Once authorisation is obtained, approval by a Justice of the Peace must be granted before the relevant surveillance activity can be undertaken. The requirement of Magistrates' approval applies to both authorisations and renewals.

8. The Senior Responsible Officer's Role

8.1 The Council's Senior Responsible Officer (SRO) is the Chief Executive.

8.2 The SRO is responsible for:

- The integrity of the process in place within the Council for the management of Covert Human Intelligence Sources and Directed Surveillance.
- Compliance with Part II of RIPA and the Codes of Practice.
- Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections.
- Oversight of the implementation of any post-inspection action plan approved by the IPCO.
- Ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports by the Investigatory Powers Commissioner's Office.
- Presenting the Council's Policy Statement on an annual basis to the designated elected Member for review.

8.3 Specific Responsibilities

8.3.1 The Senior Responsible Officer is responsible for ensuring quarterly reports are made to the Audit Governance and Standards Committee. The Committee is responsible for checking the consistency of the report with this policy and that the policy remains fit for purpose. They are not involved in making decisions on specific authorisations.

8.3.2 The Senior Responsible Officer is responsible for submitting annual statistics to the IPCO in relation to authorisations.

8.3.3. The Senior Responsible Officer is also responsible for communicating to the IPCO any unauthorised activity that might come to the attention of the authority. This must be done within 5 working days. The records, documentation, and associated documentation relating to this unauthorised activity must be retained by the Senior Responsible Officer and disclosed to the IPCO upon request, and certainly to an inspector from the IPCO at the commencement of the next scheduled inspection.

9. Records

9.1 The Senior Responsible Officer is responsible for ensuring a central register of authorisations and approvals is maintained. This is actioned through the RIPA Co-ordinating Officer.

9.2 The register and all associated documents relating to authorisations and approvals, reviews, cancellations, or renewals and refused applications should be retained in an auditable format, with each particular authorisation and approval allocated a unique reference number cross referenced to a unique reference number for that particular investigation or activity.

9.3 Records should be retained for a period of at least **three years** from the ending of the authorisation and should contain information as specified in the Code of Practice (see procedures documentation).

10. Retention and destruction of results of investigations

10.1 Material obtained in the course of criminal investigations and which may be relevant to the investigation must be recorded and retained in accordance with the Criminal Procedure and Investigations Act 1996.

10.2 The Council must have in place arrangements for the handling, storage and destruction of material obtained through the use of covert surveillance and compliance with the appropriate data protection requirements must be ensured.

10.3 The Council's Information Management Policy must be adhered to. In addition, before any authorisation is approved, advice on the handling, dissemination, copying, storage, security, retention and destruction of covert surveillance material **must** be sought from the RIPA Co-ordinating Officer and the ICT Manager, in order to ensure the Council complies with the additional safeguarding obligations contained in the relevant Home Office Codes of Practice.

11. Confidential Information

11.1 Confidential information consists of; communications subject to legal privilege, (i.e. matters arising from the confidential lawyer – client relationship), communications between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material. Special consideration must be given to authorisations that involve confidential information. If the use of surveillance may result in confidential information being acquired, the use of surveillance will be subject to a higher level of authorisation (i.e. the Chief Executive).

11.2 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of persons (whether living or dead) who can be identified from it. Examples include consultations between a health professional and a patient or information from a patient's medical records. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

11.3 Material which is legally privileged is particularly sensitive and an application for surveillance which is likely to result in the acquisition of legally privileged information should only be authorised in exceptional and compelling circumstances. The person authorising must also be satisfied that the proposed covert surveillance or property interference is proportionate to what is sought to be achieved.

11.4 If there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser within the Local Authority's legal department before any further dissemination of material takes place.

12. Grounds for Authorisation

12.1 Section 28(3) of the Act allows for authorisation for directed surveillance to be granted by an authorising officer where he/she believes that the authorisation is necessary in the circumstances of the particular case. In the case of a Local Authority the only circumstances allowed are:-

28(3) b for the purpose of preventing and detecting crime or of preventing disorder.

12.2 The authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve. "Proportionality" is defined in the Covert Surveillance and Property Interference Revised Code of Practice:-

3.6 The following elements of proportionality should therefore be considered:

- *balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;*
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

12.3 Authorisation must be given in writing.

12.4 Authorising officers should not ordinarily give authorisations in investigations or operations in which they are directly involved unless this is unavoidable.

13. Information to be provided in applications for authorisation

13.1 An application for authorisation for directed surveillance should be made in writing and should describe any conduct to be authorised and the purpose of the investigation or operation. The application should include:-

(a) the reasons why the authorisation is necessary;

(b) the grounds upon which it is sought;

(c) the reasons why the surveillance is considered proportionate to what it seeks to achieve; e.g. could the information be achieved by another means?

(d) the nature of the surveillance; e.g. where will officers be located, will they use a vehicle, what equipment will be used?

(e) the identities, where known, of those to be the subject of the surveillance;

(f) an explanation of the information which it is desired to obtain as a result of a surveillance;

(g) the details of any potential collateral intrusion and why the intrusion is justified;

(h) the details of any confidential information that is likely to be obtained as a consequence of the surveillance'

(i) the level of authority required (or recommended where that is different) of the surveillance;

(j) a subsequent record of whether authority was given or refused, by whom and the time and date.

14. Duration of authorisations

14.1 A written authorisation/approval ceases to have effect unless renewed and approved at the end of a period of three months beginning with the date on which it took effect (12 months for CHIS and 4 months for a juvenile CHIS).

15. Reviews

15.1 Authorisations should be reviewed regularly to assess the need for surveillance to continue. The results of a review should be recorded in the central record of authorisations. Particular attention should be paid to reviews where the surveillance provides access to confidential information or involves collateral intrusion.

15.2 It is the responsibility of the authorising officer to determine how often a review should take place and this should be as frequently as is considered necessary and practicable.

16. Renewals

16.1 If at any time before an authorisation would cease to have effect the authorising officer considers it necessary for the authorisation to continue for the purpose of which it was given, he may renew it in writing for a further period of 3 months. Magistrate approval must then be obtained prior to expiry of the original authorisation in order for activity to continue.

16.2 All applications for renewal of an authorisation should record:-

(a) whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

(b) any significant changes to the information contained in the original application;

(c) the reasons why it is necessary to continue the surveillance;

(d) the content and value to the investigation or operation of the information so far obtained from the surveillance;

(e) the result of regular reviews of the investigation or operation.

16.3 Renewal records should be kept as part of the central record of authorisations.

17. Cancellations

17.1 The authorising officer who granted or last renewed the authorisation must cancel it as soon as it no longer meets the criteria for which it was originally authorised. In any event, it will expire after 3 months (12 months for CHIS).

17.2 Where the authorising officer is no longer available the person who is taking over that role will be responsible.

18. Ceasing surveillance activity

18.1 As soon as the decision to cease directed surveillance is taken all those involved must be directed to stop surveillance of the subject. The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation where relevant.

19. Recording of telephone conversations

19.1 Council staff are not permitted to record telephone conversations, as such a covert activity is outside the powers of a Local Authority (see also paragraph 6.2).

20. Authorising the use of Covert Intelligence Sources

20.1 In most cases a human source that volunteers or provides information that is within their personal knowledge, without being induced, asked or tasked by a public authority, will not be a CHIS and therefore will not require authorisation. However the tasking of a person is not the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible therefore that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct.

20.2 Local Authorities are permitted to use CHIS.

20.3 A person is a CHIS if:-

(a) he establishes or maintains a personal or other relationship with a person for a covert purpose or facilitates the doing of anything within paragraph b) or c).

(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

20.4 The grounds for authorisation and approval under Section 29(3) of the Act are the same as those in S28(3) (see paragraph 12.1 above). However, only S28(3)(b) applies to Local Authorities.

20.5 In line with Section 29(5)(a) and (b) of the 2000 Act a "handler" and a "controller" will be appointed for each CHIS.

The person referred to in Section 29(5)(a) of the 2000 Act (the "handler"):-

- will have day to day responsibility for dealing with the CHIS;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

The person referred to in Section 29(5)(b) of the 2000 Act (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

The authorising officer must ensure that there is a satisfactory risk assessment in place.

20.6 Detailed records must be kept of the authorisation and approval and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation

of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records. The records kept by public authorities should be maintained in such a way as to preserve the confidentiality , or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

Particulars to be contained in records

The following matters are specified for the purposes of paragraph (d) of Section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):-

- the identity of the source;
- the identity, where known, used by the source;
- any relevant investigating authority other than the authority maintaining the records;
- the means by which the source is referred to within each relevant investigating authority;
- any other significant information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have, where appropriate, been properly explained to and understood by the source;
- the date when, and the circumstances in which, the source was recruited;
- the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in Section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under Section 29(2)(c);
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of him in relation to his activities as a source;
- all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- the information obtained by each relevant investigating authority by the conduct or use of the source;
- any dissemination by that authority of information obtained in that way; and
- in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or

provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

20.7 Vulnerable adults and minors are the subject of special provisions when used as CHIS. Authorisation will not be given for the collation of information from a CHIS under the age of 16 for the purpose of gathering information against his parents.

20.8 Where the use of a CHIS is being contemplated, the need to seek legal advice must be considered. Consideration should be given, in any case likely to place the CH IS at any risk of danger or of violence, to seeking assistance from North Yorkshire Police.

21. Internet and Social Networking sites

21.1 Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether a RIPA authorisation should be obtained.

21.2 Viewing of open source material does not require authorisation unless and until it is repeated or systematic, at which stage directed surveillance authorisation should be considered.

21.3 Passing an access control so as to look deeper into the site, for example by making a 'friend request', requires at least directed surveillance authorisation. If the investigator is to go further and pursue enquiries within the site, thereby establishing a relationship with the site host in the guise of a member of the public, this requires CHIS authorisation.

21.4 Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded or retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest.

21.5 Staff using the internet for investigative purposes must not use their own personal devices (PC, laptop, tablet, smart phone etc.). It is important to bear in mind that all internet activity leaves a 'footprint'. Websites can routinely gather IP addresses and in some cases 'data trawling' software may be used to gather more detailed information, which is then potentially traceable.

21.6 Staff must not, under any circumstances, use their own personal Social Networking Sites (SNS), profiles or other online accounts to undertake investigative research. The safety of staff is paramount and such practices could potentially put staff or their families at risk of repercussions.

22. Investigatory Powers Commissioner's Office

22.1 The Investigatory Powers Commissioner is an independent Judicial Commissioner who has oversight of the operation of the Act. Public bodies are liable to inspection on behalf of the Investigatory Powers Commissioner and have a duty to produce records and comply with requests for information made by the Investigatory Powers Commissioner or his inspectors.

23. Complaints

23.1 The Act establishes an independent tribunal which has full powers to investigate and decide on any complaint relating to the operation of surveillance regulated by the Act.

PROCEDURE FOR OBTAINING AUTHORISATION FOR DIRECTED SURVEILLANCE OR USE CHIS UNDER RIPA

DIRECTED SURVEILLANCE

1. Applying for Authorisation

1.1 Where an Investigating Officer believes that there is a need for Directed Surveillance during the course of an investigation, the Investigating Officer must complete an Application for Authority for Directed Surveillance [see appendix 2] after discussion with his line manager, if appropriate.

1.2 The completed form must be submitted to the Authorising Officer [see appendix 1 for departmental Authorising Officers].

2. Granting Authorisation/Obtaining Magistrate Approval

2.1 The Authorising Officer can only approve an application where the statutory grounds for doing so are met.

2.2 Where the Authorising Officer is satisfied that the criteria for granting an authorisation are met, he will approve the application and return a copy of the endorsed application to the Investigating Officer. The Investigating Officer must then obtain approval from a Justice of the Peace, using the specified form and supplying the required authorisation documentation, before the required surveillance activity can take place. A Legal Officer will also attend court to assist with this process. The Authorising Officer may also be required to attend. Once approval has been obtained, the Authorising Officer will set the first review date and specify the expiry date in accordance with the prompts provided on the authorisation forms (3 months less one day for directed surveillance; 12 months less one day for CHIS; 4 months less one day for a juvenile CHIS).

2.3 The Authorising Officer will arrange for the original application and approval documentation to be included within the central register of authorisations, i.e. by passing them to the RIPA Co-ordinating Officer

2.4 The RIPA Co-ordinating Officer will record the above information within the register held for that purpose.

3. Reviewing Authorisation

3.1 The Authorising Officer, in granting the Authorisation, will endorse it with a review date. At the review the Investigating Officer will complete the Review of Directed Surveillance Authorisation form [see appendix 2] for consideration by the Authorising Officer. The Authorising Officer is responsible for determining whether the grounds for continued surveillance remain. If so, the Authorising Officer will grant the application. Otherwise, it will be refused.

3.2 It is recommended that authorisations are reviewed on at least a monthly basis.

3.3 The Authorising Officer will arrange for the original application to be included within the central register of authorisations, i.e. by passing them to the RIPA Co-ordinating

Officer. Reviews are monitored and recorded by the RIPA Co-ordinating Officer in the register held for that purpose.

4. Refusing Authorisation

4.1 Where the Authorising Officer is not satisfied that the criteria for granting authorisation for directed surveillance are met, he will refuse the application and endorse the application accordingly. The documents will then be passed to the RIPA Co-ordinating Officer.

5. Cancelling Authorisation

5.1 Any activity authorised under RIPA must be kept under review. Where surveillance is completed the Investigating Officer will complete a Cancellation of Directed Surveillance form [see appendix 2] and forward it to the Authorising Officer for approval.

5.2 The Authorising Officer will arrange for the cancellation to be included within the central register of authorisations, i.e. by passing the document to the RIPA Co-ordinating Officer.

6. Renewal

6.1 Authorisations last for a maximum of 3 months in the first instance and must be renewed if surveillance is to continue beyond this time limit. The Investigating Officer is responsible for ensuring that any application for an extension is made in a timely manner.

6.2 Where it is necessary to extend authorisation the Investigating Officer will complete a Renewal of Directed Surveillance Authorisation form [see Appendix 2] and forward it to the Authorising Officer for approval. The Investigating Officer must then obtain approval for the extension from a Justice of the Peace, using the specified form and supplying the required authorisation documentation, before the expiry of the original authorisation in order for the activity to continue.

6.3 The Authorising Officer will arrange for the original application and renewal approval documentation to be included within the central register of authorisations i.e. by passing them to the RIPA Co-ordinating Officer.

7. Retention of Authorisation Records

7.1 The Senior Responsible Officer will retain records relating to authorisations under RIPA for 3 years from the date authorisation was granted or renewed.

COVERT HUMAN INTELLIGENCE SOURCES

9.1 Applications, Reviews, Cancellations and Extensions apply in relation to CHIS as above, and there are separate forms applicable to such applications [see appendix 2].

9.2 The Authorising Officer should not grant any such application without first seeking legal advice from the RIPA Co-ordinating Officer or in his absence the Council's Deputy Monitoring Officer. In considering such an application the Authorising Officer must have rather to that advice, to this Practice and Procedure guidance, and (as applicable) to the relevant Code of Practice guidance issued by the Home Office entitled 'Covert Surveillance and Property Interference', 'Covert Human Intelligence Sources', 'Protection of Freedoms Act 2012' (see Appendix 2).

APPENDIX 1

LIST OF DESIGNATED PERSONS AND AUTHORISING OFFICERS

Senior Responsible Officer & Authorising Officer	-	Chief Executive
RIPA Co-ordinating Officer & Authorising Officer	-	Director of Law and Governance
Authorising Officer	-	Deputy Chief Executive
Authorising Officer	-	Director of Finance
	-	
	-	
	-	
	-	
	-	
	-	
	-	

In any matter involving “Confidential Information” or the authorisation of a vulnerable individual or a juvenile as a CHIS, the Chief Executive is required to act as the Authorising Officer.

APPENDIX 2

RIPA FORMS

All forms can be downloaded from:

https://www.gov.uk/government/collections/ripa-forms--2

It is your responsibility to ensure that you are using the current version of the RIPA forms. If in doubt – seek advice from the RIPA Co-ordinating Officer.

The form to be used for applications for Magistrate approval, in both the Directed Surveillance and CHIS sections is at:

http://.www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

Directed Surveillance

1. Application for Directed Surveillance Authorisation
2. Review of Directed Surveillance Authorisation
3. Cancellation of Directed Surveillance Authorisation
4. Renewal of Directed Surveillance Authorisation
5. Magistrate approval of authorisation/renewal.

Cover Human Intelligence Sources

6. Application for use of CHIS
7. Review of CHIS Authorisation
8. Cancellation of CHIS Authorisation
9. Renewal of CHIS Authorisation
10. Magistrate approval of authorisation/renewal.

Please also see:

Home Office Guidance to Local Authorities, at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

In particular, the application process to the Magistrates is explained from page 10 onwards.

Codes of Practice

The Home Office Codes of Practice are available by following the link below.

https://www.gov.uk/government/collections/ripa-codes

It is your responsibility to ensure that you have considered the relevant parts of the relevant Code of Practice. If in doubt – seek advice from the RIPA Co-ordinating Officer.

Appendix C

HAMBLETON DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000

DIRECTED SURVEILLANCE CENTRAL AUTHORISATION REGISTER

RIPA No:	Name and Location:	Description of Operation:	Authorisation Type:	"URN Authorisation"	Officer Authorising (and Grade/Rank and whether Directly Involved in Investigation):	Date Authorised Internally:	Self Authorised Y/N:	Date Approved by Magistrate	Likely to Reveal Confidential Information?	Expiry Date of 3 Months	Review Date:	Renewal Details (when, who, grade/rank)	Cancellation Date	Destruction Date for Material	Officer Responsible for Destruction

Authorisation Type: O = Original Authorisation
R = Renewal Authorisation
A = Amendment