CABINET – 10TH FEBRUARY 2022

Report of the Head of Strategic Support
Lead Member: Councillor Margaret Smidowicz

Part A

ITEM 14 REGULATION OF INVESTIGATORY POWERS ACT: POLICY AND REVIEW OF USE DURING 2021

Purpose of Report

To approve a Regulation of Investigatory Powers Act (also known as RIPA, or the 2000 Act) Policy, and consider a summary of the use of RIPA during 2021.

Recommendations

1. That it be noted that there has been no use of RIPA by the Council during the calendar year 2021.

2. That the Audit Committee be requested to continue its responsibility for receiving a quarterly report on the use of RIPA, and to report to Cabinet any concerns arising from those reports that may indicate that the use of RIPA is not consistent with the Policy or that the Policy may not be fit for purpose.

3. That the updated RIPA Policy Statement 2022, attached as Appendix A to this report, be approved.

Reasons

1. To ensure compliance with the requirements of the Home Office's current 'Code of Practice – Covert Surveillance and Property Interference' relating to the involvement of elected Members in approving the RIPA policy and reviewing the Council's use of RIPA on at least an annual basis.

2. To ensure compliance with the requirements of the Home Office's latest 'Code of Practice – Covert Surveillance and Property Interference' relating to elected Members considering reports on the use of RIPA on at least a quarterly basis to ensure that is it being used consistently with the policy and the policy remains fit for purpose.

3. To ensure that the Council's RIPA Policy Statement remains up to date and consistent with the relevant legislation and codes of practice.

Policy Justification and Previous Decisions

The use of RIPA to conduct covert surveillance in appropriate instances may support many of the Council's enforcement and anti-fraud policies. The Home Office Code of Practice, which relevant bodies are obliged to follow when using RIPA, requires that elected Members should set a RIPA policy on an annual basis.

Implementation Timetable including Future Decisions and Scrutiny

The Audit Committee will continue to receive regular quarterly monitoring reports on any use of RIPA by the Council.

Report Implications

The following implications have been identified for this report.

Financial Implications

None.

Risk Management

There are no identified risks associated with the decision Cabinet is asked to make.

Key Decision:	No
Background Papers:	None
Officer to contact:	Adrian Ward (01509) 634573 adrian.ward@charnwood.gov.uk

Part B

Background

1. RIPA provides for the authorisation of covert surveillance by the Council where that surveillance is likely to result in the obtaining of private information about a person.

2. Surveillance includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. Surveillance is covert if it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

2. The Council only has the power to authorise covert surveillance under RIPA for the purpose of preventing or detecting crime, or of preventing disorder.

3. RIPA applications are required to be approved by a Justice of the Peace (JP) at the Magistrates' Court in addition to an internal authorisation process. The Protection of Freedoms Act 2012 requires that local authority authorisations and notices under RIPA for the use of particular covert investigation techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP). This would require the Council to make a formal application to a Magistrates' Court, followed by a hearing at Court in private at which the application for a surveillance order may be granted or declined by the Magistrates.

4. A local authority can only obtain an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are:

   - Criminal offences which attract a custodial sentence of six months or more; or
   - Certain criminal offences under sections 146, 147 or 147A of the Licensing Act 2003 involving the sale of alcohol to children; or
   - Certain criminal offences under section 7 of the Children and Young Persons Act 1933 relating to the sale of tobacco to minors.

5. Examples of offences which would not meet the above conditions are:

   - Any fine-only offences, such as littering, dog fouling or a householder failing the duty of care to check that household waste taken for disposal was taken by a person authorised to transfer waste (section 34 of the Environmental Protection Act 1990).
   - Any offences attracting a penalty of less than 6 months imprisonment, for instance false representations for obtaining benefit (s. 112 of the Social Security Administration Act 1992), which has a maximum penalty of 3 months imprisonment.

6. Examples of offences which would meet the above conditions are any offence attracting a penalty of 6 months or more imprisonment, such as:
   - Fly tipping (section 33 of the Environmental Protection Act 1990), which has a penalty of up to 5 years imprisonment.
   - Offences given special status under RIPA (as amended), such as the selling of alcohol or tobacco to children.

7. The requirements around the RIPA authorisation process are complex, and the Home Office has responsibility for issuing a Code of Practice under the Act to specify the processes and procedures which must be followed. The Code of Practice includes a best practice requirement that:

   'Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose', (s3.35).

8. The Cabinet is therefore responsible for receiving an annual overall report on the use of RIPA and for approving the RIPA policy each year, and the Audit Committee are responsible for receiving quarterly reports on the use of RIPA and for reporting back to Cabinet any concerns relating to potential inconsistency with the policy, or if the policy does not appear to be fit for purpose.

9. The Council received an inspection report by the Investigatory Powers Commissioner's Office (IPCO) in September 2021 (attached as Appendix B) which made some recommendations regarding updating the RIPA policy, which have been incorporated into the policy statement that Cabinet are being asked to approve (Appendix A).

Appendices

Appendix A: RIPA Policy Statement (February 2022)
Appendix B: IPCO inspection report

APPENDIX A

CHARNWOOD BOROUGH COUNCIL

COVERT SURVEILLANCE

REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY STATEMENT

(February 2022)

Policy Statement
Regulation of Investigatory Powers Act 2000

Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a legal framework for covert surveillance activities by public authorities (including local authorities). The Investigatory Powers Commissioner's Office (IPCO) operates as an independent inspector to monitor these activities.

The use of surveillance (both overt and covert) to provide information is a valuable resource for the protection of the public and the maintenance of law and order. To discharge their responsibilities local authorities and law enforcement agencies use unaided surveillance and surveillance devices. RIPA and codes of practice under it provide a legal framework and procedure to authorise the use of covert surveillance. Surveillance is covert if it is carried out in a manner that is calculated to ensure that people who are subject to is are unaware that it is or may be taking place.

In some circumstances, it may be necessary for Council employees, in the course of their duties, to make observations of people in a covert manner. Actions of this sort may constitute an interference with a person's right to privacy. This may give rise to legal challenge as a potential breach of "the right to respect for private and family life" under Article 8 of the European Convention on Human Rights and the Human Rights Act 1998. RIPA provides a procedure to defend the Council against such challenges.

Purpose

This policy statement is designed to ensure that Charnwood Borough Council meets the legal requirements in relation to the use of covert surveillance. It also promotes a professional approach in undertaking surveillance so that those affected may have confidence that the Council will act effectively and in a fair and lawful manner. It should be read in conjunction with the Regulation of Investigatory Powers Act 2000 and the current versions of the Code of Practice on the use of Covert Human Intelligence sources and the Code of Practice on Covert Surveillance.

STATEMENT OF INTENT

This policy statement applies only to the use of covert surveillance, although it is expected that usually any surveillance activity undertaken by or on behalf of the Council will be overt.

The Council will fulfil its lawful obligations and use directed surveillance within the terms of the Regulation of Investigatory Powers Act 2000 and the directions of the IPCO.

The Council will keep its policy and procedures under review and update them as necessary and in accordance with any changes in the law.

The Council will take necessary steps to ensure that all employees and councillors are aware of all relevant policy standards, procedures, legislation and best practice. Employees have a duty to follow this policy and its procedures and any employee acting outside this policy will be subject to the Council's disciplinary procedures.

Evidence gathered by surveillance will be treated as confidential and will only be disclosed to persons (internal and external) whose authority has been explicitly established. Such evidence may only be removed by employees from a Council office with the authority of their Head of Service of another senior officer formally designated by the Head of Service. Employees will be responsible for any misuse, security breach of unauthorised disclosure while such evidence is in their control.

Evidence gathered by covert surveillance will be held for as long as the law requires (a minimum of 5 years) after which it may be destroyed in a secure manner.

The Council will keep in place appropriate security measures as required.

Appropriate physical security will be provided for visitors being received and supervised at all times within the Council offices where evidence gathered by surveillance is stored.

Each service will be responsible for the security of evidence collected by it. Security arrangements will be reviewed regularly. All reported breaches or potential weaknesses will be investigated by the Head of Service concerned and where necessary further or alternative measures introduced.

A reporting structure will be established headed by the RIPA Monitoring Officer with a liaison officer in each service so that authorisation, review, renewal and cancellation forms and procedures are:

- co-ordinated and consistent, and
- available for inspection by the IPCO;

and so that any problems can be identified and investigated.

The intention is that subjects of covert surveillance carried out by or on behalf of the Council can be assured that evidence collected (including personal data) will be processed with care and in accordance with the law.

Council employees will not carry out intrusive surveillance within the meaning of the Regulation of Investigatory Powers Act 2000. This is covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle; and involves the presence of an individual or a device on the premises or in the vehicle, or by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

Although the law does not impose a requirement on the Council to seek or obtain authorisations, it will seek to adhere to the authorisation, review, renewal and cancellation procedure provided for by RIPA and the codes of practice before conducting any covert surveillance. The Council will not gather evidence by covert surveillance of individuals where it is disproportionate or unnecessary in relation to the purposes of the investigation.

Surveillance carried our by a third party on behalf of the Council shall be subject to a contract which stipulates compliance with the law and this policy.

PRINCIPLES OF SURVEILLANCE

In planning and carrying out covert surveillance Council employees shall comply with the following principles:

Lawful Purposes

Directed surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (see section 28(3) of RIPA) available to local authorities, namely;

a) for the purposes of preventing or detecting crime or the prevention of disorder.

Employees carrying out surveillance shall not interfere with any property or harass any person.

Confidential Material

Applications where a significant risk of acquiring confidential material has been identified shall always require the authorisation of the Chief Executive (or in his absence a Director) after consulting with the RIPA Monitoring Officer.

Confidential material consists of;

- matters subject to legal privilege (eg. between a professional advisor and client)
- confidential personal information (eg. relating to a person's spiritual, physical or mental health), or
- confidential journalistic material.

DEFINITIONS

Unless the context otherwise requires, in this document the expressions in the first column shall have the meaning in the second column and any reference to a statute or statutory instrument or code of practice within the document shall include amendments to it.

Authorising Officer	means a person entitled to give an authorisation for directed surveillance or for the use of a covert human intelligence source in accordance with section 30 of RIPA and the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order SI. No. 2417, as adapted to the organisational structure of the Council and who is included in the list of officers designated as such by the Council within the Delegations to Officers section of the Council's Constitution.
Council	means Charnwood Borough Council
Covert Human Intelligence Source (CHIS)	means a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within sections 26(8)(b) or (c) of RIPA, namely: (b) to covertly use such a relationship to obtain information or to provide access to any information to another person; or (c) to covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence or such a relationship
Covert Surveillance	means surveillance carried out in a manner that is calculated to ensure that persons who are subject to this surveillance are unaware that it is or may be taking place
Directed Surveillance	means covert surveillance which is not intrusive and is undertaken; (a) for the purpose of a specific investigation or a specific operation, (b) 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 (c) 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 RIPA to be sought for carrying out the surveillance
Private Information	means information about a person relating to his or her private or family life
Private Vehicle	means any vehicle that is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it
Residential Premises	means so much of any premises as is for the time being occupied or used by any person, however temporarily, as living accommodation (including hotels or prison accommodation that is being so occupied or used)
Social Media	means websites and applications that enable users to create and share content or to participate in social networking (eg. Twitter and Facebook)
Surveillance Device	means any apparatus designed or adapted for use in surveillance
Surveillance *	is defined in section 48 of RIPA, and includes: (a) monitoring, observing or listening to persons, their movements, their conversations or their activities or communications, (b) recording anything monitored, observed or listened to in the course of the surveillance, and (c) surveillance by or with the assistance of s surveillance device * surveillance does not include

	references to: (a) any conduct of a covert human intelligence source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source, (b) the use of a covert human intelligence sources for so obtaining or recording information, or (c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services, or Part III of the Police Act 1997 (powers of the police and of customs officers)
Necessity	means that the use of covert surveillance is considered to be necessary, and that there are no other suitable means or processes which can be applied to obtain the information required
Proportionality	means that the following considerations must have been applied: (a) balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence (b) explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others (c) 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 (d) evidencing, as far as reasonably practicable, what

	other methods have been considered and why they were not implemented.

SCOPE OF PROCEDURE

The procedure does not apply to:

- Observations that are not carried out covertly, or
- Ad-hoc covert observations that do not involve the systematic surveillance of a specific person(s)
- Unplanned observations made as an immediate response to events.

In cases of doubt, the authorisation procedure described below should be followed.

AUTHORISATION PROCEDURE

General

All directed surveillance and the use of covert human intelligence sources must be for a purpose that is necessary and proportionate to enable the Council to perform its duties and services and is subject to the inspection of the IPCO.

Authorisation will be obtained using the forms based on the current Home Office Model and approved by the Council's RIPA Monitoring Officer.

Forms, codes of practice and supplementary material will be available on the Council's intranet and will be maintained by the RIPA Monitoring Officer.

Applications for directed surveillance will only be made to an Authorising Officer. Officers responsible for management of an investigation will normally be no lower than a Team Leader and will not be graded below Senior Officer grade.

Authorising Officers will be at least Head of Service level, and will be trained to properly understand the requirements of RIPA. Authorising Officers should avoid authorising their own activities wherever possible and only do so in exceptional circumstances. An alternative Authorising Officer will otherwise be the Authorising Officer for such activities.

Authorising Officers shall ensure they are fully aware of their responsibilities and comply with the requirements of the law including the requirement to obtain magistrate's approval, the relevant codes of practice and the Council's policies and procedures in respect of the authorisation, review, renewal and cancellation of authorisations for covert surveillance.

Where an application for authorisation is refused, the Authorising Officer shall record the refusal on the application and the reasons for it on the case file and supply a copy of it to the RIPA Monitoring Officer as with other authorisations as quickly as possible and in any event within 7 days. The Authorising Officer shall also ensure that any supplementary information and supporting

documents submitted with any application for authorisation, review, renewal or cancellation are recorded and retained on the case file as required by the codes of practice or other legal requirement.

Consideration needs to be given at the start of the investigation as to whether or not the criminal offence that is being investigated meets the threshold criteria for RIPA authorisations:

- Criminal offences which attract a custodial sentence of six months or more; or
- Certain criminal offences under sections 146, 147 or 147A of the Licensing Act 2003 involving the sale of alcohol to children; or
- Certain criminal offences under section 7 of the Children and Young Persons Act 1933 relating to the sale of tobacco to minors.

If the Authorising Officer is satisfied that these criteria have been met then a further form requesting authorisation by the Magistrates' Court must be completed and sent to the Court together with a completed copy of the internal RIPA authorisation and any other appropriate evidence to support the application. Prior to this a hearing date must be listed with the Leicester Magistrates' Court for hearing the application by a Justice of the Peace.

Guidance on the process for obtaining Magistrate's authorisation can be obtained from the RIPA Monitoring Officer, and is available on the relevant section of the Council's intranet.

The effective authorisation period only commences once magisterial concurrence is given.

Directed Surveillance

All applications for directed surveillance authorisation will be made on **Form 1** (reference *RIPA 1 DS authorising* form). The applicant in all cases should complete this, and approval must be obtained from an Authorising Officer and from a magistrate. In urgent cases there are arrangements in place for out of hours approval to be obtained from a magistrate.

All applications for review of directed surveillance authorisation will be made on **Form 2** (reference *RIPA 2 DS review* form). The applicant in all cases should complete this where the investigation/operation is to be continued or cancelled.

All applications for directed surveillance renewals will be made on **Form 3** (reference *RIPA 3 DS renewal* form). The applicant in all cases should complete this where surveillance requires to continue beyond the previously authorised period (including previous renewal). As well as approval from an Authorising Officer, Magistrates approval is required for all renewals.

Where authorisation ceases to be either necessary or appropriate the Authorising Officer will cancel an authorisation using **Form 4** (reference *RIPA 4 DS cancellation* form).

Any person giving an authorisation for the use of directed surveillance must record on the appropriate form the matters they took into account in reaching their decision and they must be satisfied that:

- no overt means are suitable for the purpose
- the authorisation is for a prescribed lawful purpose
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated/targeted in the operation or investigation (collateral intrusion)
- measures are being taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion
- the authorisation is necessary
- the proposed surveillance is proportionate and any equipment to be used is specified.

Necessity
Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Effectiveness
Surveillance operations shall be undertaken only by suitably trained employees (or under their direct supervision). The Authorising Officer will determine which employees are to be involved in an operation and ensure that they are suitably trained.

Proportionality
The use of surveillance shall not be excessive but shall be in proportion to the significance/harm of the matter being investigated. Consideration of proportionality will be based on the factors set out in the Definitions section of this policy.

Authorisation
All directed surveillance shall be authorised in accordance with this procedure. Care must be taken by Authorising Officers to ensure that each authorisation is completed in its entirety by them, and in handwriting.

Use of a Covert Human Intelligence Source (CHIS)

Proper records must be kept of the authorisation and use of a source as required by Regulation 3 of Regulation of Investigatory Powers (Source Records) Regulations 2000, namely:

(a) the identity of the source
(b) the identity, where known, used by the source
(c) any relevant investigating authority other than the authority maintaining the records
(d) the means by which the source is referred to within each relevant investigating authority
(e) any other significant information connected with the security and welfare of the source
(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in (e) above 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
(g) the date when, and the circumstances in which, the source was recruited

(h) 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 RIPA or in any order made by the Secretary of State under section 29(2)(c)
(i) the periods during which those persons have discharged those responsibilities
(j) the tasks given to the source and the demands made of him or her in relation to the activities as a source
(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority
(l) the information obtained by each relevant investigating authority by the conduct or use of the source
(m) any dissemination by that authority of information obtained in that way, and
(n) 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 of 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.

In addition, the Code of Practice requires records to be kept of:

- a copy of the authorisation together with the supporting documentation and notification of the approval given by the Authorising Officer
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- the reason why the person renewing the authorisation considered it necessary to do so
- any risk assessment made in relation to the source
- the circumstances in which tasks were given to the source
- the value of the source to the investigating authority
- a record of the results of any reviews of the authorisation
- the reasons why, if any, for not renewing an authorisation
- the reasons for cancelling an authorisation
- the date and time when any permission was given by the Authorising Officer to cease using a source.

Authorising Officers must not grant an authorisation for a CHIS unless they believe that there are arrangements in place to ensure at all times there is a person responsible for maintaining a record of the use of that source, and that the person responsible is fully aware of their duty of care towards, and the safeguarding of, the CHIS.

Only the Chief Executive, or in his absence a Strategic Director, may authorise the use of a juvenile or vulnerable CHIS. In such instances the authorisation can be for a maximum period of 4 months, and must be subject to a review of the authorisation at least monthly.

All applications for authorisation for the use or conduct of a CHIS will be made on **Form 5** (reference *RIPA 5 CHIS authorising* form). The applicant in all cases should complete this. All applications need to be approved by a Magistrate as well as by an Authorising Officer.

All applications for review of authorisation for the use or conduct of a CHIS will be made on **Form 6** (reference *RIPA 6 CHIS review* form). The applicant in all cases should complete this where the investigation/ operation is to be continued or cancelled.

All applications for authorisation for the use or conduct of a CHIS renewals will be made on **Form 7** (reference *RIPA 7 CHIS renewal* form). The applicant in all cases should complete this where the surveillance requires to continue beyond the previously authorised period (including a previous renewal). As well as approval from an Authorising Officer, Magistrates approval is required for all renewals.

Where authorisation ceases to be either necessary of appropriate the Authorising Officer will cancel an authorisation using **Form 8** (reference *RIPA 8 CHIS cancellation* form).

Forms and other relevant material will be available on the Council's intranet and will be maintained by the RIPA Monitoring Officer.

Any person giving an authorisation for the use of CHIS must record on the appropriate form matters taken into account in reaching their decision and must be satisfied that:

- no overt means are suitable for the purpose
- the authorisation is for a prescribed lawful purpose
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated/targeted in the operation or investigation (collateral intrusion)
- measures are being taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion
- the authorisation is necessary
- the proposed surveillance is proportionate and any equipment to be used is specified.

<u>Necessity</u>
Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

<u>Effectiveness</u>
Surveillance operations shall be undertaken only by suitably trained or experienced employees (or under their direct supervision). The Authorising Officer will determine which employees are to be involved in an operation and ensure that they are suitably trained.

<u>Proportionality</u>
The use of surveillance shall not be in excess but shall be in proportion to the significance/harm of the matter being investigated. Consideration of proportionality will be based on the factors set out in the Definitions section of this policy.

<u>Authorisation</u>
All directed surveillance shall be authorised in accordance with this procedure. Care must be taken by Authorising Officers to ensure that each authorisation is completed in its entirety by them, and in handwriting.

DURATION TIME OF AUTHORISATIONS

Authorisations

Written authorisations for directed surveillance expire after 3 months, starting on the day from which they took effect.

Written authorisations for the use of a CHIS expire after 12 months beginning on the day on which they took effect, except for a juvenile CHIS where the expiry period will be 4 months.

Renewals

If at any time before an authorisation expires, an Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 months for directed surveillance of 12 months for a CHIS (or 4 months for a juvenile CHIS), in each case starting on the day on which the previous authorisation ceases to have effect. Applications should only be made approximately two weeks before the authorisation is due to expire, as this will allow time for a magistrate's approval to be sought. In the case of a CHIS, a review must be carried out immediately beforehand.

Authorising Officers may renew authorisations more than once, provided they continue to meet the criteria for authorisation.

Renewals must be approved by a magistrate.

Review

Authorising Officers shall review all authorisations at regular intervals or not more than one month. In the case of a CHIS the review shall be as frequently as considered necessary and practicable and include: the use made of the source during the period authorised, the tasks given to the source and the information obtained. Details of the review and the decision reached shall be noted on the original application.

Cancellation

Authorising Officers must cancel an authorisation if they are satisfied that the need for it no longer satisfies the criteria for authorisation or, additionally in the case of a CHIS, that satisfactory arrangements for the source's case no longer exist. Where necessary, the safety and welfare of the CHIS shall continue to be taken into account after the authorisation has been cancelled.

SAFEGUARDS (including privileged or confidential information)

The Council must ensure that any information it obtains through surveillance (or via a CHIS) is handled in accordance with the safeguards the Council has

put in place, any relevant frameworks (such as data protection), and the Home Office Codes.

Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. Something is necessary for the authorised purposes where the material:

(a) is (or is likely to become) necessary for the surveillance purposes set out in the legislation;
(b) is necessary for facilitating the carrying out of the functions of the Council under the surveillance legislation;

(c) is necessary for facilitating the carrying out of any functions of the Commissioner or Investigatory Powers Tribunal;

(d) is necessary for the purposes of legal proceedings; or

(e) is necessary for the performance of the functions of any person by or under any enactment.

When information obtained under a surveillance authorisation is used evidentially, the Council should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements.

All information and material obtained through surveillance and all copies, extracts or summaries must be stored securely to minimise the risk of theft or loss. Only those with appropriate legal authority and security clearance should be able to access the information.

The Council will ensure that it has in place:

(a) physical security to protect premises where the information is stored or can be accessed;

(b) IT security to minimise risk around unauthorised access to IT systems;

(c) An appropriate security clearance regime to provide assurance that those who have access to the information are reliable and trustworthy.

SOCIAL MEDIA

RIPA implications must be considered in relation to the use of social media sites (such as Twitter and Facebook) for gathering evidence to assist in enforcement activities, as set out below:

- officers must not create a false identity in order to ‘befriend’ individuals on social media networks without authorisation under RIPA

- officers viewing an individual's public profile on a social media network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation
- repeated viewing of open profiles on social media networks to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been obtained
- officers should be aware that it may not be possible to verify the accuracy of information on social media networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

RECORD KEEPING, TRAINING AND MONITORING

Security and Retention of Records

Each service or discrete location within a service which makes use of RIPA must maintain a record of all applications for authorisations (including refusals), renewals, reviews and cancellations on the appropriate forms. Each individual form will be given a unique central reference number by the RIPA Monitoring Officer, although services may also allocate their own investigation or operation numbers as well. The unique central reference number should follow on in sequential order from the used for previous forms. The lead officer in each service responsible for the investigation or operation will maintain progress record sheets for directed surveillance and CHISs.

Documents created under this procedure are confidential and shall be treated as such. Services shall make appropriate arrangements for their retention, security and destruction in accordance with RIPA and the codes of practice. In the case of a CHIS, special care will be taken to preserve the confidentiality of any source and information provided by them.

The Authorising Officer shall retain, together, the original authorisation, review and renewal forms until cancelled. On cancellation, the original forms and any associated documents shall be retained in a secure place for at least 5 years after cancellation.

All completed RIPA forms must be submitted to the RIPA Monitoring Officer as soon as possible, and in any event, within 7 days of their completion. This will include forms which have resulted in an authorisation being refused.

Training

The RIPA Monitoring Officer will be responsible for ensuring that RIPA training for the Senior Responsible Officer and Authorising Officer takes place and must retain a record of all training undertaken. Refresher training will be provided at intervals of no more than 2 years.

Central Register

The RIPA Monitoring Officer will maintain the central register of authorisations. Authorising Officers shall notify the RIPA Monitoring Officer as soon as reasonably practicable of the grant, renewal and cancellation of any

authorisation and the name of the applicant officer to ensure the accuracy of the central register. They shall send on a regular monthly basis a signed and dated photocopy of any authorisation (including refusals), renewals, reviews and cancellation forms for directed surveillance and similarly for those for the use of a CHIS.

The RIPA Monitoring Officer

The Council has designated an officer to act as the RIPA Monitoring Officer (currently the Head of Strategic Support). The RIPA Monitoring Officer will have responsibility for keeping an oversight of the Council's RIPA administration arrangements, and in particular:

- for organising RIPA training within the Council,
- raising awareness of RIPA and its regulatory framework amongst officers and Members, for example by maintaining appropriate guidance on the Intranet and by publishing articles about RIPA in internal publications,
- maintaining the Central Record of Authorisations, and
- Examining submitted RIPA documents to ensure they are of the required standard.

The Senior Responsible Officer

The Council has designated the Strategic Director of Corporate Services to act as the Senior Responsible Officer, who is responsible for:

- the integrity of the process in place within the Council for the management of CHIS and Directed Surveillance;
- compliance with Part 2 of the Act and with the Codes;
- engagement with the IPCO inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

The Authorising Officers

The Council's designated authorising officers are:

- Chief Executive
- Strategic Director of Corporate Services
- Head of Customer Experience, and
- Head of Neighbourhoods and Communities.

Elected Members

Elected Members:

- should review the Authority's use of the RIPA and set the policy at least once a year,
- should also consider reports on the use of RIPA Act on at least a quarterly basis to ensure that is it being used consistently with the policy and the policy remains fit for purpose,
- they should not however be involved in making decisions on specific authorisations.

The Investigatory Powers Commissioner's Office (IPCO)

The IPCO provides an independent overview of RIPA powers. This scrutiny includes inspection visits to local authorities by inspectors appointed by the IPCO.

RIPA established an independent tribunal. This tribunal has full powers to investigate and decide any cases within its jurisdiction.

The Council will ensure that copies of the Tribunal's information sheet, their complaint form and their Human Rights Act claim form will be made available at the Council's main offices. These and the relevant codes of practice produced by the Home Office will be made available on the Council's intranet.

ADVICE

Further advice about covert surveillance will be provided by the RIPA Monitoring Officer. In particular, advice should be sought before considering the use of a CHIS where the considerations of risk assessment, duty of care and safeguarding responsibilities, insurance, managing the source and ensuring confidentiality require specific consideration.

FURTHER INFORMATION AND ENQUIRIES

The RIPA Monitoring Officer is the first point of contact on any of the matters raised in this policy statement. Enquiries should be addressed to:

The RIPA Monitoring Officer
Head of Strategic Support
Charnwood Borough Council
Southfields Road
Loughborough
LE11 2TX

Tel: (01509) 634573

The RIPA Monitoring Officer will be responsible for dealing with all internal and external enquiries.

HOME OFFICE CODES OF PRACTICE

The Home Office have produced Codes of Practice which give guidance on the use of covert surveillance and covert human intelligence sources by public

authorities under part 2 of RIPA 2000. They are available via the following link:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

COMPLAINTS

Any complaints relating to the Council's use of RIPA or the application of this policy statement should be in writing, dated and include details of the complaint and also an account of the nature of the problem, and should be sent to:

The Chief Executive
Charnwood Borough Council
Southfields Road
Loughborough
LE11 2TX

The Council will attempt to complete internal investigations within 20 working days. An acknowledgement of the complaint will be sent as soon as possible after its receipt.

APPENDIX B

IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Mr Robert Mitchell
Chief Executive
Charnwood Borough Council
Southfield Rd
Loughborough
LE11 2TN

Rob.Mitchell@charnwood.gov.uk

2 September 2021

Dear Mr Mitchell,

Inspection of Charnwood Borough 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.

Your Council was recently the subject of a virtual inspection by one of my Inspectors, REDACTED . I am grateful to Mr Adrian Ward, your Head of Strategic Support and RIPA Monitoring Officer, for taking the lead in this discussion and providing all the relevant documentation. Mr Simon Jackson, your Strategic Director for Environmental Services also joined the discussion in his capacity as RIPA Senior Responsible Officer (SRO).

As a result of the inspection REDACTED has made a number of recommendations which are detailed below, and I would be grateful if they could be addressed at the earliest opportunity:

Covert Surveillance Policy

Your policy has recently been presented to and agreed by Elected Members, which is good to see. The policy is generally well written and covers many of the required elements well. As the key reference point for staff considering whether any proposed activity requires authorisation under RIPA, you may wish to follow the route that many councils have taken by including simple flow charts which guide the reader through the initial considerations, application process and include any necessary signposting.

While your policy recognises the impact of the IP Act and the existence of IPCO, there are still several references to one of its precursor organisations (OSC) which should be removed. Authorisation periods are included in the policy but the variation when considering the authorisation of a Juvenile Covert Human Intelligence Source should also be made clear.

Data Assurance

In the absence of any surveillance product, the inspection sought reassurance that the necessary measures were in place to manage such product should it ever be captured. Your current policy refers to the management of product and surveillance records but does not cover all the safeguarding requirements outlined in the current Home Office Codes of Practice for surveillance and CHIS. Your RIPA policy should be amended to reflect those requirements, and you may consider an addition to your Central Record to monitor the management of any such product.

Senior Responsible Officer

Mr Jackson seems aware of his responsibility as SRO but by his own admission, very much relies on Mr Ward to manage any RIPA related enquiries and issues, while his priorities lay elsewhere. Mr Ward has provided reassurance that any identified issues will be escalated appropriately to the SRO, aided by the fact that Mr Jackson is his immediate line manager. It is somewhat concerning that internally, beyond Mr Ward, there is little knowledge of RIPA across the organisation, which adds weight to the next paragraph.

Training and awareness

I note you have not conducted any training for some time. While this is not ideal, I do understand that training budgets are somewhat limited and bearing in mind Charnwood Borough Council has not conducted any RIPA activity in recent times, RIPA training could easily slip down the list of priorities. That said, many RIPA errors occur because of the lack of knowledge, and therefore some method of raising awareness across the organisation should be implemented. This would seem to have been highlighted by a recent letter received in my Office from one of your Elected Members. The letter not only highlighted a lack of awareness of the legislation but more importantly, a lack of understanding of where to go to seek advice internally. The letter was nonetheless responded to accordingly and the appropriate advice given.

In conclusion, although your Council is a limited user of its surveillance powers, I take the opportunity here to reiterate to you the importance of regular, ongoing internal oversight of the actual or potential use of these powers, which should be managed through your Senior Responsible Officer.

I hope that you find this letter to be helpful and constructive. My Office is available to you should you have any queries following the recent inspection, or at any point in the future. Contact details are provided at the foot of this letter.

I shall be grateful if you would acknowledge receipt of the report within two months and let me know your plans in regard to the compliance matters identified herein.

Yours sincerely,

SIGNATURE REDACTED

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