



Additional / To Follow Agenda Items

This is a supplement to the original agenda and includes reports that are additional to the original agenda or which were marked 'to follow'.

Nottingham City Council Executive Board

Date: Tuesday, 18 July 2023

Time: 2.00 pm

Place: Ground Floor Committee Room - Loxley House, Station Street, Nottingham, NG2 3NG

Governance Officer: Phil Wye **Direct Dial:** 0115 8764637

Agenda

Pages

- 4 Regulation of Investigatory Powers (RIPA) Policy**
Report of the Portfolio Holder for Finance and HR

3 - 22

This page is intentionally left blank

NOTTINGHAM CITY COUNCIL

REGULATION OF INVESTIGATORY POWERS

ACT 2000 (RIPA)

POLICY AND GUIDANCE ON PART II

CONTENTS

1. Policy
2. Guidance – Part II – Direct Surveillance and Covert Human Intelligence Source
3. Appendix A – Links to Home Office - Forms
4. Appendix B – Links to Home Office - Codes of Practice
5. Appendix C – NCC Online Research and Investigation Guidance

NOTTINGHAM CITY COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Nottingham City Council only carries out covert surveillance where such an action is justified and endeavours to keep such surveillance to a minimum. It recognises its obligation to comply with RIPA when such an investigation is for one of the purposes set out in that Act and has produced this Guidance document to assist officers.

Applications for authority

A senior officer of at least the level of Head of Service or equivalent authorised by the Council will consider all applications for authorisation in accordance with RIPA. Any incomplete or inadequate application forms will be returned to the applicant for amendment. The authorising officer shall in particular ensure that:-

- There is a satisfactory reason for carrying out the surveillance
- Any directed surveillance passes the “serious crime” threshold
- The covert nature of the investigation is necessary
- Proper consideration has been given to collateral intrusion
- The proposed length and extent of the surveillance is proportionate to the information being sought
- Chief Executive’s authorisation is sought where confidential legal/ journalistic/ medical/ spiritual welfare issues/ parliamentary issues are involved
- The authorisations are reviewed and cancelled
- Records of all authorisations are sent to the Information Compliance Team Leader for entry on the Central Register and copies are sent to legal for a hard-copy central register.

Training

The Information Compliance team shall be responsible for the training of applicants and Authorising Officers.

Each Authorising Officer will then ensure that relevant members of staff are aware of the Act’s requirements.

The Senior Responsible Officer shall ensure that refresher training is offered once a year to all Directorates of the Council and also to require the legal team and the Information Compliance team to give advice and training on requests.

Central register and records

The Information Compliance Team Leader shall retain the Central Register of all authorisations issued by Nottingham City Council. The Information Compliance Team Leader, together with the Criminal Solicitors in Legal, will also monitor the content of the application forms and authorisations to ensure that they comply with the Act.

Senior Responsible Officer

The Senior Responsible Officer, a role required by IPCO with oversight of Local Authority's use of part II powers, is the Director of Legal and Governance, Mr Malcolm R Townroe.

RIPA Coordinating Officer

The Information Compliance Team leader, presently Naomi Matthews, will perform the RIPA Coordinating Officer role, with responsibility for the day-to-day RIPA management and administrative processes observed in obtaining an authorisation and advice thereon.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

GUIDANCE ON PART II

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1. Purpose

The purpose of this guidance is to explain:

- (i) the scope of RIPA – Part II,
- (ii) the circumstances where it applies, and
- (iii) the authorisation procedures to be followed

2. Introduction

- 2.1 This Act, which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer before they are carried out.
- 2.2 The investigatory powers, which are relevant to a local authority, are directed covert surveillance in respect of specific operations, involving criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco, and the use of covert human intelligence sources. The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are also Codes of Practice in relation to the use of these powers and the Home Office web site links for these are at **Appendix B.**
- 2.3 Consideration must be given, prior to authorisation as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be gleaned in other ways.

3. Definitions

- 3.1 'Covert' is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place. (s.26(9)(a))
- 3.2 'Covert human intelligence source' (CHIS) is defined as a person who establishes or maintains a relationship with a person for the covert purpose of obtaining information about that person. (s.26 (8))

- 3.3 'Directed surveillance' is defined as covert but not intrusive and undertaken:
- (i) for a specific investigation or operations,
 - (ii) in such a way that is likely to result in the obtaining of private information about any person,
 - (iii) other than by way of an immediate response (s.26 (2))
- 3.4 'Private information' includes information relating to a person's private or family life.
- 3.5 'Intrusive' surveillance is 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 using a surveillance device. **Nottingham City Council may not authorise such surveillance.**
- 3.6 An Authorising Officer must be the Chief Executive, Head of Service, Director, Head of Legal Services, a Corporate Director, Director or Head of Service (or equivalent) responsible for the management of an investigation (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI No. 521)). An Authorising Officer will have undergone training to support them in this role and the Council's Information Compliance Team will retain a list of approved Authorising Officers. The Senior Responsible Officer is the Director of Legal and Governance. The role of the Senior Responsible Officer is to oversee the compliance of the Authorising Officers and processes in use in Nottingham City Council.
- 3.7 The Senior Responsible Officer will authorise and maintain a list of Authorising Officers and Investigating Officers. The Council's Information Compliance Team will retain this list.

4. Scrutiny and Tribunal

4.1 External Scrutiny

- 4.1.1 The Investigatory Powers Commissioners Office (IPCO) was set up to monitor compliance with RIPA. IPCO has "a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA", and the Surveillance Commissioner will from time to time inspect the Council's records and procedures for this purpose.
- 4.1.2 As of 1st November 2012, the Council has to obtain an order from a Justice of Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity carried out. The Council can only appeal a decision of the Justice of the Peace on a point of law by Judicial Review.

- 4.1.3 In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. Applications will be heard on a Judicial Review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.
- 4.1.4 The Tribunal can order:
- Quashing or cancellation of any warrant or authorisation,
 - Destruction of any records or information obtained by using a warrant or authorisation,
 - Destruction of records or information held by a public authority in relation to any person.
- 4.1.5 The Council has a duty to disclose to the tribunal all documents they require if any Council officer has:
- Granted any authorisation under RIPA
 - Engaged in any conduct as a result of such authorisation.

4.2 Internal Scrutiny

- 4.2.1 The Council will ensure that at all times the Senior Responsible Officer is responsible for;
- the integrity of the process in place within the Council to authorise directed surveillance and CHIS
 - Compliance with Part II of the Act and with the accompanying Codes of Practice
 - Engagement with the Commissioners and inspectors when they conduct their inspections
 - Overseeing the implementation of any post-inspection action plans or recommendations as suggested by the Inspector/Commissioner.
- 4.2.2 The elected members of the Council will review the Authority's use of the Act and the Authority's policy and guidance documents at least once a year. They will also consider internal reports on the use of the Act on at least a quarterly basis to ensure that it is being used consistently with the Local Authority's policy and that the policy remains fit for purpose. The Elected Members will not however be involved in making decisions with regards to specific authorisations.

5. Benefits of RIPA authorisations

- 5.1 The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, RIPA provides a defence to an accusation of an infringement of a human right by creating a statutory framework under which covert surveillance can be authorised and conducted compatibly with

Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

- 5.2 Material obtained through properly authorised covert surveillance may be admissible evidence in criminal proceedings.

6. When does RIPA apply?

- 6.1 Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS, is necessary for the purpose of preventing or detecting crime.
- 6.2 The Council can only authorise **directed surveillance** to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or be an offence under:-
- a) S.146 of the Licensing Act 2003 (sale of alcohol to children)
 - b) S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
 - c) S.147A of the Licensing Act 2003 (persistently selling alcohol to children)
 - d) S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen)

CCTV

- 6.3 The normal use of CCTV is not usually covert because members of the public would normally require authorisation to view CCTV and are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV covertly and in a pre-planned manner as part of a specific investigation or operation to target a specific individual or group of individuals. Equally a request, say by the police, to track particular individuals via monitoring CCTV recordings may require authorisation (from the police). This policy should be read in conjunction with NCC CCTV policy.

7. Covert Human Intelligence Source

- 7.1 The RIPA definition (section 26) is anyone who:
- a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b) or c)
 - b) covertly uses such a relationship to obtain information or provide access to any information to another person; or
 - c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Any reference to the conduct of a CHIS includes the conduct of a source which falls within a) to c) or is incidental to it.

References to the use of a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

7.2 Section 26(9) of RIPA goes on to define:-

- b) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and
- c) a relationship is used covertly, and information obtained as mentioned in subsection (8)(c) above and is disclosed covertly, if, and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

7.3 There is a risk that an informant who is providing information to the Council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised in the 2000 Act, not whether or not the CHIS is asked to do so by the Council. When an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship, it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on any information from such an informant.

7.4 Juvenile Sources

7.4.1 Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility for him. The duration of a juvenile CHIS is one month. The Regulation of Investigatory Powers (Juveniles) Order 2000 SI No. 2793 contains special provisions which must be adhered to in respect of juvenile sources.

7.5 Vulnerable individuals

7.5.1 A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances.

8. Authorisations

8.1 Applications for directed surveillance

8.1.1 All application forms must be fully completed with the required details to enable the Authorising Officer to make an informed decision.

No authorisation shall be granted unless the Authorising Officer is satisfied that the investigation is:

- necessary for either the purpose of preventing or detecting crime or of preventing disorder,
- Involves a criminal offence punishable whether summarily or on indictment by a maximum sentence of at least six months imprisonment or related to the underage sale of alcohol or tobacco (see para 6.2 for offences),
- proportionate to the ultimate objective. This has 3 elements, namely 1) that the method of surveillance proposed is not excessive to the seriousness of the matter being investigated, 2) the method used must be the least invasive method available to ensure the target's privacy, 3) the privacy of innocent members of the public must be respected and collateral intrusion minimised (see 8.1.2).
- and that no other form of investigation would be appropriate.

The grant of authorisation should indicate that consideration has been given to the above points and if there are any areas of concern these should be discussed with the Information Compliance Team specialist or Legal Services. The following however are crucial points that should be adhered to in every case;

Necessity: Covert surveillance cannot be said to be necessary if the desired information can reasonably be obtained by overt means. It must also be necessary for the purpose of preventing or detecting crime.

Proportionality: The method of surveillance proposed must not be excessive in relation to the seriousness of the matter under investigation. It must be the method which is the least invasive of the target's privacy.

Collateral intrusion which affects the privacy rights of innocent members of the public, must be minimised and use of the product of the surveillance carefully controlled so as to respect those rights.

8.1.2 The Authorising Officer must also take into account the risk of 'collateral intrusion' i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation, particularly where there are special sensitivities e.g. premises used by lawyers, doctors or priests e.g. for any form of medical or

professional counselling or therapy. The application must include an **assessment** of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any unnecessary intrusion.

Those carrying out the investigation must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

8.1.3 Special consideration in respect of confidential information

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy, e.g. where confidential information is involved.

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

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Information Compliance Team leader and/or Legal Services should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the Codes of Practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 of the Freedom of Information Act.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive, or, in his absence, a Chief Officer and should only be authorised where there are exceptional and compelling circumstances that make authorisation necessary.

8.1.4 Notifications to Inspector/Commissioner

The following situations must be brought to the Inspector/Commissioner's attention at the next inspection:

- Where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved,
- Where a lawyer is the subject of an investigation or operation;
- Where confidential personal information or confidential journalistic information has been acquired and retained.

8.1.5 Special considerations in respect of social networking sites

The fact that digital investigations are routine or easy to conduct does not reduce the need for authorisation if the criteria are met. Any surveillance carried out on the internet must be carried out in accordance with the Nottingham City Council's policy and guidance on internet investigations (see Appendix C).

8.1.6 Applications for CHIS

This process is the same as for directed surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least 6 months in imprisonment does not apply. The authorisation must specify the activities and identity (by pseudonym only) of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

A risk assessment and record must be prepared and records need to be kept for this purpose.

All application forms must be fully completed with the required details to enable the authorising officer to make an informed decision.

8.1.7 Judicial Approval of authorisations

Once the Authorising Officer has authorised the Directed Surveillance or CHIS, the Investigating Officer who completed the application form should contact the Magistrates Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The Investigating Officer will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

In addition the Investigator will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the Officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate and whether that continues to be the case. They will also consider whether the authorisation was given by the appropriate designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

The Justice of the Peace can:

- (a) **Approve the grant of the authorisation**, which means the authorisation will then take effect.
- (b) **Refuse to approve the grant of the authorisation**, which means the authorisation will not take effect but the Council could look at the reasons for refusal, make any amendments and reapply for judicial approval.
- (c) **Refuse to approve the grant of the authorisation** and quash the original authorisation. The Court cannot exercise its power to quash the authorisation unless the applicant has at least two business days from the date of the refusal in which to make representations.

8.1.7 Working in Partnership with the Police and other agencies

Authorisation can be granted in situations where the Police or other agency rather than Nottingham City Council require the surveillance to take action, as long as the behaviour complained of, meets all criteria to grant and in addition is

also of concern to the Council. Authorisation cannot be granted for surveillance requested by the police or other agency for a purely police or other agency purpose. Where the Authority is authorising the surveillance under RIPA, all required documentation must be completed by Council Officers.

Where another agency or organisation has an existing relationship with Nottingham City Council, any covert surveillance carried out by them must be under a RIPA obtained by Nottingham City Council and the authorisation must be subject to the safeguards as if Nottingham City Council carried out the surveillance.

9. Unique Operation Reference Numbers

Each application for Directed Surveillance and CHIS must have a Unique Reference Number (URN). This URN will begin with **2NCC** for a Part II Nottingham City Council surveillance application, followed by the year in which the authority was granted followed by a sequential number, for example 2NCC/10/01.

10. Duration and Cancellation

- An authorisation for **directed surveillance** shall cease to have effect (if not renewed or cancelled) 3 months from the date the Justice of the Peace approves the grant.
- If renewed the authorisation shall cease to have effect 3 months from the expiry date of the original authorisation.
- An authorisation for **CHIS** shall cease to have effect (unless renewed or cancelled) 12 months from the date the Justice of the Peace approves the grant or renewal.

This does not mean that the authorisation should necessarily be permitted to last for the whole period so that it lapses at the end of this time. The authorising officer, in accordance with section 45 of the Act, must cancel each authorisation as soon as that officer decides that the surveillance should be discontinued. Documentation of any instruction to cease surveillance should be retained and kept with the cancellation form.

On cancellation the cancellation form should detail what product has been obtained as a result of the surveillance activity. The form should include the dates and times of the activity, the nature of the product obtained and its format, any associated log or reference numbers, details of where the product is to be held and the name of the officer responsible for its future management.

11. Reviews

The Authorising Officer should review all authorisations at intervals determined by him/herself. A review date should always be set by the Authorising Officer. This should be as often as necessary and practicable (usually monthly). The reviews should be recorded using the review forms and copies of these sent to Information Compliance Team for monitoring and central recording.

Particular attention should be paid to the possibility of obtaining confidential information and an assessment as to the information gleaned should take place at each review.

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals. It would be appropriate to call a review specifically for this purpose.

12. Renewals

Any authorised officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect. The renewal must then be approved by the Justice of the Peace in the same way the original authorisation was approved. The process outlined in paragraph 8.1.7 should be followed for renewals.

A CHIS authorisation must be thoroughly reviewed before it is renewed.

13. Central Register of authorisations

13.1 All authorities must maintain the following documents:

- Copy of the application and a copy of the authorisation form and the approval order from the Magistrates together with any supplementary documentation and notification of the approval given by the authorised officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the authorising officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation and supporting documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the authorising officer (including an instruction to cease surveillance).

13.2 To comply with 13.1, the Information Compliance Team Leader holds the central register of all authorisations issued by officers of Nottingham City Council. The original of every authorisation, review, renewal and cancellation issued should be lodged immediately with the Information Compliance Team Leader. A copy should however be kept both by the applicant and Authorising Officer and any relevant review dates noted in their respective diaries. Any original authorisations and renewals taken to the Magistrates Court should be retained by the Council the Court must only keep copies of the authorisations or renewals.

13.3 The Council must also maintain a centrally retrievable record of the following information:

- type of authorisation;
- date the authorisation was given;
- date the approval order was given by the Justice of the Peace;
- name and rank/grade of the authorising officer;
- unique reference number of the investigation/operation;
- title (including brief description and names of the subjects) of the investigation/operation;
- details of renewal;
- dates of any approval order for renewal given by the Justice of the Peace;
- whether the investigation/operation is likely to result in obtaining confidential information;
- whether the authorisation was granted by an individual directly involved in the investigation ;
- date of cancellation.

These records will be retained for at least 3 years and will be available for inspection by the Office of Surveillance Commissioners.

14. Retention of records

All documents must be treated as strictly confidential and the Authorising Officer and the Local Authority must ensure that arrangements are in place for the secure retention, handling, storage and destruction of material obtained through the use of surveillance under RIPA. The Authorising Officers through the Information Compliance Team Officer must ensure compliance with the Council's Data Protection Policy, the UK General Data Protection Regulation 2016/679 and

the Data Protection Act 2018, RIPA and the RIPA Codes of Practice and any relevant practices relating to the handling or storage of materials.

15. Complaints procedure

- 15.1 The Council will maintain the standards set out in this guidance and the Codes of Practice (**See Appendix B**). IPCO has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.
- 15.2 Contravention of the UK General Data Protection Regulation 2016/679 and the Data Protection Act 2018 may be reported to Information Commissioners office (ICO). Before making such a reference, a complaint concerning a breach of this guidance should be made using the Council's own internal complaints procedure. To make a complaint about this type of matter please contact the Data Protection Officer, Nottingham City Council, Loxley House, Station Street, Nottingham NG2 3NG or telephone 0115 8764415.

APPENDIX A

Forms

See Home Office website:

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

APPENDIX B

Codes of Practice

See Home Office website:

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

APPENDIX C

NCC Online Research and Investigation Policy

See link:

[..\NCC RIPA Online Research and Investigation Policy V1 - final
version.docx](#)

This page is intentionally left blank