Appendix A

(November 2021)

North Tyneside Council

Covert Surveillance Policy

(Regulation of Investigatory Powers Act 2000) (RIPA)

1. INTRODUCTION

This is North Tyneside Council's Covert Surveillance Policy document. It sets out the adopted approach of the Authority to ensure that any surveillance activity undertaken by the Authority is conducted in a way that is compatible with the human rights of individuals, in particular the right to respect for private and family life (in accordance with Article 8 of the European Convention on Human Rights).

The aim of the Policy is to:

- Explain the Authority's arrangements for authorising surveillance activity;
- Direct Officers to the key sources of guidance to ensure compliance with the Policy;
- Give effect to the rights of citizens to respect for their private and family lives (pursuant to the Human Rights Act 1998);
- Protect the Authority from legal challenge when undertaking surveillance; and
- Assist the Authority in complying with the Codes of Practice, Regulations and Orders issued under the Regulation of Investigatory Powers Act 2000 (RIPA) and to meet the requirements of the Inspectors from the Investigatory Powers Commissioner's Office (IPCO).

2. POLICY STATEMENT

The Authority agrees that as a matter of policy:

- The Authority is committed to complying with:
  (a) the Regulation of Investigatory Powers Act 2000 (RIPA) and the Codes of Practice issued under RIPA by the Home Office; and
  (b) guidance supplied by the Investigatory Powers Commissioner's Office (IPCO);
- Surveillance that falls outside of the RIPA regime will be subject to the Non-RIPA authorisation procedure and central monitoring to ensure:
  (a) the Authority has an overview of all surveillance activity it undertakes;
  (b) such activity is appropriately scrutinised; and
  (c) the rights of individuals are appropriately safeguarded.
- Relevant Officers shall receive sufficient training and guidance so as to reasonably ensure such compliance;
- Any Officer shall, if in any doubt about whether the legislation applies in a particular case or how to comply with it, seek guidance from an Authorising Officer and/or the Head of Law and Governance.

3. REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework under which covert surveillance activity can be authorised and conducted in a way that is compatible with the rights of individuals. Where RIPA is complied with it provides statutory protection from legal challenge to the local authority and for this reason it is often referred to as the "RIPA shield".

Three covert investigatory techniques are available to local authorities under RIPA:

i. directed surveillance – covert surveillance of individuals in public places e.g. to tackle criminal activity;
ii. covert human intelligence sources (CHIS) such as the deployment of undercover officers; and

iii. the acquisition and disclosure of communications data such as telephone billing information or subscriber details e.g. to tackle rogue traders.

The Authority will use RIPA authorised surveillance where appropriate in order to detect and prevent crime. Authorisation will only be given where the proposed surveillance is both necessary and proportionate. The Protection of Freedoms Act 2012 requires local authorities to obtain the prior approval of a Justice of the Peace before the use of any one of the three covert investigatory techniques available as detailed above. An approval is also required if an authorisation to use such techniques is being renewed.

In each case, the role of the Justice of the Peace is to ensure that the correct procedures have been followed and the relevant factors have been taken into account. Approval can only be given if the Justice of the Peace is satisfied that:

a) There were reasonable grounds for the Authority's Authorising Officer approving the application to believe that the Directed Surveillance or deployment of a CHIS was necessary and proportionate and that there remain reasonable grounds for believing so;
b) The Authorising Officer was of the correct seniority within the organisation i.e. a Head of Service, Service Manager or equivalent in accordance with the relevant Regulations;
c) The granting of the authorisation was for the prescribed purpose of preventing or detecting crime and satisfies the Serious Offence Test for Directed Surveillance (see below); and
d) Any other conditions set out in any order under Part 2 of RIPA are satisfied (there are none at present).

In addition to the above, where the authorisation is for the deployment of a CHIS, the Justice of the Peace must be satisfied that:

a) the local authority can ensure that there are officers in place to carry out roles relating to the handling and management of the CHIS as well as the keeping of records;
b) Where the CHIS is under 16 or 18 years of age, the necessary requirements in relation parental consent, meetings, risk assessments and the duration of the authorisation have been satisfied. Note that the authorisation of such persons to act as a CHIS must come from the Head of Paid Service.
c) Where the application is for the renewal of a CHIS authorisation, a review has been carried out by the local authority and the Justice of the Peace has considered the results of the review. The provisions in relation to judicial approval make it clear that the Authorising Officer is not required to apply in person and there is no need to give notice to either the subject of the authorisation or their legal representatives. This reflects the covert nature of the exercise of the investigatory powers under RIPA. The Authority would be represented in any application to a Justice of the Peace by the Authority's Legal Service and the Authorising Officer. There is no requirement for a Justice of the Peace to consider either cancellations or internal reviews of authorisations.

At all times the risk of obtaining private information about persons who are not subjects of the surveillance must be considered (collateral intrusion) and steps must be taken to avoid or minimise it.

Examples of investigations where it is envisaged that covert techniques may be utilised to enable local authorities to gather evidence and offer evidence in legal proceedings include:

- Trading Standards e.g. action against loan sharks and rogue traders, car fraud, consumer scams, deceptive advertising, counterfeit goods, unsafe toys and electrical goods; and

- Environmental protection e.g. action to stop large scale waste dumping, the sale of unfit food etc.

Serious Offence Test

Local authorities may only use the RIPA provisions to authorise surveillance activities in order to detect and prevent crime as defined by the Regulations. In particular the crime which is sought to be prevented or detected by the surveillance activity must be 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, section 7 of the Children and Young Persons Act 1933 and sections 91 and 92 of the Children and Families Act 2014. The latter are all offences involving sale of tobacco and alcohol to underage children.

4. NECESSARY AND PROPORTIONATE

The Authority may only authorise directed surveillance, CHIS or the acquisition of communications data where it is both necessary and proportionate to what it seeks to achieve. Senior Offices are appointed as Authorising Officers (or Designated Persons for communications data purposes) and have a key role to play in carefully scrutinising all applications. Authorising Officers/Designated Persons must ensure that authorisations are granted only in appropriate cases and that the extent of all authorisations are clearly set out.

5. COLLATERAL INTRUSION

Collateral intrusion is obtaining private information about persons who are not subjects of the surveillance. The risk of collateral intrusion must be considered, and measures should be taken to avoid or minimise it.

6. NON-RIPA SURVEILLANCE

Surveillance activity which falls outside of RIPA, for example, monitoring of employees, does not benefit from the RIPA shield. When operating outside of the RIPA regime there is a greater risk of breaching an individual's rights or being successfully challenged.

The Authority via its Senior Responsible Officer retains a central register of Non-RIPA surveillance activity. Officers are required to take great care to appropriately record, authorise, monitor and scrutinise such activity.

The principles of proportionality and necessity and the requirement to avoid or minimise collateral intrusion also apply to Non-RIPA surveillance.

7. CLOSED CIRCUIT TELEVISION (CCTV) SYSTEMS

Overt surveillance via CCTV is covered by the Data Protection Act 2018 and not by RIPA. CCTV is subject to the Surveillance Camera Code of Practice under the Data Protection Act, which is overseen by the Surveillance Camera Commissioner.
Signage must be in place to inform the public when they enter zones covered by CCTV equipment.

A central record of all CCTV in buildings operated by the Authority is held by the Senior Responsible Officer.

If CCTV cameras are used for covert surveillance (whether by the Authority or the Police), a RIPA authorisation is required.
North Tyneside Council's CCTV control room operates cameras throughout the North Tyneside area. The Police may make formal written requests for surveillance of a target for which they have a RIPA authorisation. Confirmation by sight of this authorisation will be sought and a copy will be retained (redacted as appropriate) by the CCTV Control Room Co-Ordinator.

Employees using CCTV covertly must be aware of the possibility of collateral intrusion (invading the privacy of people other than the target) and take steps to avoid or minimise it.

The Protection of Freedoms Act 2012 makes provision for the further regulation of surveillance camera systems. These are defined as Closed Circuit Television (CCTV), Automatic Number Plate Recognition (ANPR) and other surveillance camera technology.

The Surveillance Camera Code of Practice also includes guidance in relation to the development or use of such systems, and the use and processing of information derived from them. The Code of Practice includes provisions about:

- considerations as to whether to use surveillance camera systems;
- types of systems or apparatus
- technical standards for systems or apparatus
- locations for systems or apparatus
- the publication of information about systems or apparatus
- standards applicable to persons using or maintaining systems or apparatus
- standards applicable to persons using or processing information obtained by virtue of systems
- access to, or disclosure of, information so obtained
- procedures for complaints or consultation

The Authority must have regard to the Code if they operate or intend to operate any surveillance camera systems covered by the Code.

Failure to adhere to the Code will not in itself render an organisation liable to legal proceedings, but the Code is admissible in civil or criminal proceedings. The Code could also be enforced by way of judicial review in the High Court.

The CCTV provisions in the Protection of Freedoms Act 2012 add a completely new layer of control over the use of CCTV by local authorities.

8. CORPORATE RESPONSIBILITIES

The Authority's Senior Responsible Officer (currently the Head of Law and Governance) has overall responsibility for RIPA.

The Senior Responsible Officer appoints Authorising Officers and Designated Persons. A list of Authorising Officers/Designated Persons is held with the Central Record. This list may change as required. Only Authorised Officers named in the list may authorise covert surveillance activities under RIPA. Only Designated Persons named in the list may authorise the acquisition of communications data. The Senior Responsible Officer may remove an Officer from the list where they consider it is appropriate to do so.

In particular, the Senior Responsible Officer ensures that:

- Only Officers who have received appropriate training on RIPA are permitted to become Authorising Officers/Designated Persons.
- Refresher training is provided as required and training records are maintained.
- Monitoring arrangements are in place in each Service to ensure that the Authority is meeting its obligations under RIPA, the Codes of Practice, and this Policy.
- Reviews of authorisation documentation take place to ensure that they are completed in accordance with the requirements of RIPA, the Codes of Practice and Authority guidance. Appropriate feedback is given to officers to ensure high standards are encouraged and maintained.
- The Central Record is maintained in accordance with the requirements of the Codes of Practice and Authority guidance.
- An up-to-date copy of this Policy and associated guidance is available to all relevant employees.
- An annual review of this Policy is undertaken and presented to Cabinet for approval, in addition to provision of monitoring information.

The RIPA Co-ordinating Officer (currently the Information Governance Manager – Information Governance) supports the Senior Responsible Officer in relation to the discharge of that role. The RIPA Co-ordinating Officer also monitors all authorisations and provides robust challenge to authorisations to ensure they meet the requirements of the law and this Policy.

Each Head of Service is responsible for ensuring effective and legally compliant systems and procedures are in place for surveillance work within their Service Areas in respect of any surveillance activity whether undertaken within or outside of the RIPA provisions.

The Senior Responsible Officer is also responsible for ensuring that:

- Relevant officers receive appropriate training on RIPA before undertaking investigations that include (or may include) Directed Surveillance, the use of a CHIS or the acquisition or disclosure of communications data.
- Refresher training is provided as required and training records are maintained and supplied to the Senior Responsible Officer.
- Authorisations are approved, reviewed, renewed, and cancelled by the Authorising Officer/Designated Person as necessary, and such actions are reported to the Senior Responsible Officer.
- Records and evidence obtained as a result of surveillance/investigation are kept and destroyed in accordance with Authority Policy.

All employees connected with surveillance and handling evidence are responsible for ensuring that they act only in accordance with their level of responsibility and training and in accordance with this Policy and associated documents.

9. GUIDANCE

The Authority's intranet has a surveillance page containing the key guidance documents, including this Policy, the Employee Handbook, the relevant Codes of Practice, a guide to completing RIPA forms and a link to the Home Office RIPA forms.

The Authority has prepared the 'Employee Handbook: Use of Covert Surveillance & Covert Human Intelligence Sources & Communications Data (Regulation of Investigatory Powers Act

2000 (RIPA))' to provide guidance to Authority Officers regarding the use of RIPA and the procedures that must be followed.
The Employee Handbook may be revised by the Senior Responsible Officer during the year to reflect changes in procedures or best practice.

All Authority Officers who may authorise or undertake surveillance work must read the Handbook and follow the procedures within it.

Authority Officers are encouraged to seek guidance on the procedures from the Authorising Officers/Designated Persons and the Senior Responsible Officer.

If Officers wish to undertake surveillance which falls outside of the RIPA regime they must seek appropriate authorisation. This is covered in the Employee Handbook. Information regarding surveillance (whether under RIPA or not) must be held centrally by the Senior Responsible Officer to enable the Authority to have an overview of all surveillance activities being undertaken.

10. COMPLIANCE AND OVERSIGHT

The Senior Responsible Officer will assess compliance with this policy and associated guidance. The Senior Responsible Officer may seek support from Internal Audit as appropriate.

A random sample of authorisations will be checked monthly by the Senior Responsible Officer and on receipt by the RIPA Co-Ordinating Officer and any incorrect or incomplete authorisations will be reported to the relevant Authorising Officer and Head of Service. In addition to the sample checks the Senior Responsible Officer will provide feedback and guidance to Officers as needed throughout the year.

Elected Members have a key role in setting policy and overseeing the use of RIPA within the Authority. Members do not make investigatory/enforcement casework decisions in relation to specific authorisations.

The Elected Mayor is designated to champion compliance with RIPA within the Authority processes. The Elected Mayor receives regular updates from the Senior Responsible Officer regarding the use of the Authority's powers.

The Senior Responsible Officer presents reports to Regulation & Review Committee at least annually on the Authority's use of the powers but will also usually report the use of RIPA to the

next available committee meeting. The Committee looks at compliance, oversight and use of RIPA. The Committee considers whether the policy remains fit for purpose and will recommend changes where appropriate for Cabinet's consideration.

Cabinet will receive an annual report upon the Authority's use of the powers and will set the policy for the following year.

The Authority has designated a Cabinet Member (currently the Elected Mayor) and a Senior Responsible Officer (currently the Head of Law and Governance) to champion and oversee compliance with this Policy and associated procedures. Each Head of Service is responsible for ensuring compliance with RIPA in their service area.

Cabinet will review the RIPA policy and the Authority's use of RIPA on an annual basis.

11. REVIEW OF THIS POLICY

The Senior Responsible Officer will review this policy and associated controls as follows:

- Annually.
- Following legislative changes.
- Following any recommendations received as a result of inspections and reviews undertaken by the Investigatory Powers Commissioner's Office.
- Following any major breach in compliance.

12. RECORD KEEPING

Authorising Officers must send the originals of all applications, reviews, renewals and cancellations to the Senior Responsible Officer for filing with the Central Record. In light of the confidential nature of the data original documents should be hand delivered and must be stored securely. Documentation must not be altered in any way following its completion. If any clarification is needed regarding the content of a document this must be done via a separate document which must be signed and dated.

All documentation received as a result of an authorisation must be handled and stored securely and in line with data protection principles.

13. DESTRUCTION OF MATERIAL

Any material obtained during covert surveillance that is wholly unrelated to the operation and where there is no reason to believe that it will be relevant to future civil or criminal proceedings will be destroyed immediately.

In North Tyneside Council the retention period for the central record and associated material is six years from the end of each authorisation or the conclusion of connected court proceedings (whichever date is last).

Where the retention period has expired, the authorisation and any other material obtained or created during the course of the covert surveillance under the unique reference number will be destroyed.

The Authorising Officer/Designated Person will be responsible for ensuring that all material held in the department relating to the unique reference number is destroyed.

The Authorising Officer/Designated Person will notify the Senior Responsible Officer that the retention period has expired, giving the unique reference number and authorise destruction of the material held in the Central Record of Authorisations.

All material to be destroyed will be treated as confidential waste.
Officers should also refer to the Authority's Record Retention Guidelines before destroying any document or evidence obtained under RIPA.

Further guidance on record keeping is available in the Codes of Practice.

14. TRAINING

The Senior Responsible Officer will train the senior managers responsible for overseeing and monitoring RIPA activities, all other employees involved in RIPA activities, and ensure that they understand this Policy.

The Senior Responsible Officer will keep a record of the training undertaken by employees.

15. CODES OF PRACTICE & RELATED AUTHORITY DOCUMENTS

The following Codes of Practice have been issued by the Home Office:
1. Code of Practice - Covert Surveillance and Property Interference
2. Code of Practice - Covert Human Intelligence Sources
3. Code of Practice - Acquisition and Disclosure of Communications Data

All employees involved in surveillance activities must have regard to and act in accordance with:

- the Codes of Practice;
- the Employee Handbook: Use of Covert Surveillance & Covert Human Intelligence Sources & Communications Data (Regulation of Investigatory Powers Act 2000) (RIPA); and
- instruction and guidance from Authorising Officers/Designated Persons and the Senior Responsible Officer.

The Employee Handbook includes appendices providing detailed guidance to assist in the completion of RIPA forms.

16. MISCONDUCT

All employees involved in RIPA activities will comply with this Policy. Failure to comply with this Policy may be dealt with as misconduct or gross misconduct under the disciplinary procedures depending upon all of the circumstances of the case.

17. COMPLAINTS

Any complaint made to the Authority will be dealt with in accordance with the corporate complaints procedure.