Public Document Pack

North Tyneside Council

Regulation and Review Committee

Wednesday, 13 October 2021

Thursday, 21 October 2021 The Chamber, Quadrant, The Silverlink North, Cobalt Business Park, NE27 0BY. **commencing at 6.00 pm**.

Agenda Item **Page**

1. **Apologies for Absence**

   To receive apologies for absence from the meeting.

2. **Appointment of Substitute Members**

   To be notified of the appointment of any Substitute Members.

3. **To receive any Declarations of Interest and Notification of any Dispensations Granted**

   You are invited to declare any registerable and/or non-registerable interests in matters appearing on the agenda, and the nature of that interest.

   You are also invited to disclose any dispensation in relation to any registerable and/or non-registerable interests that have been granted to you in respect of any matters appearing on the agenda.

   Please complete the Declarations of Interests card available at the meeting and return in to the Democratic Services Officer before leaving the meeting.

4. **Minutes** **3 - 4**

   To agree the minutes of the meeting held on 22 October 2020.

5. **Annual Review of Council Policy on Court Surveillance** **5 - 22**

Circulation overleaf …

Members of the Regulation and Review Committee

Councillor Jim Allan
Councillor Trish Brady
Councillor Brian Burdis
Councillor Julie Cruddas
Councillor John Hunter (Deputy Chair)
Councillor Maureen Madden
Councillor Tommy Mulvenna (Chair)
Councillor Pat Oliver
Councillor John Stirling
Councillor Lewis Bartoli
Councillor Sean Brockbank
Councillor Debbie Cox
Councillor Cath Davis
Councillor Gary Madden
Councillor Janice Mole
Councillor John O'Shea
Councillor Alan Percy
Councillor Judith Wallace

Regulation and Review Committee

Thursday, 22 October 2020

Present: Councillor J Stirling (Chair)
Councillors J Allan, L Bartoli, S Brockbank, D Cox, J Cruddas, E Darke, C Davis, N Huscroft, M Madden, J Mole, T Mulvenna and J O'Shea

Apologies: Councillors G Madden and A Percy

RQ10/20 Appointment of Substitute Members

There were no substitute members reported.

RQ11/20 To receive any Declarations of Interest and Notification of any Dispensations Granted

There were no declarations of interest or dispensations reported.

RQ12/20 Minutes

Resolved that the minutes of the meeting of Regulation and Review Committee held on 9 January 2020 be confirmed as a correct record and signed by the Chair and the minutes of the Regulation and Review Panel meetings held on 16 January 2020, 13 February 2020, 19 March 2020, 16 July 2020, 27 August 2020 and 8 October 2020 be noted.

RQ13/20 Annual Review of Council Policy on Court Surveillance

The Committee received a report in relation to the Annual Review of Council Policy on Court Surveillance. In accordance with the Codes of Practice applying to the Regulation of Investigatory Powers Act 2000 (RIPA) the Authority's Policy was subject to annual review. A copy of the draft Policy for 2021 was appended to the report.

RIPA placed covert surveillance on a statutory basis and enabled certain public authorities, including local authorities, to carry out surveillance operations with statutory protection from legal challenge. This protection was often referred to as the "RIPA shield". RIPA provisions could only be used to authorise surveillance activities to detect and prevent serious crime and the two authorising officers of the Authority were required to seek judicial approval from the Magistrates' Courts before any surveillance was undertaken.

The Members were informed that three covert techniques were available to local authorities under RIPA:

- The acquisition and disclosure of communication data such as telephone billing information or subscriber details e.g. to tackle rogue traders

- Direct surveillance – covert surveillance of individuals in public places e.g. to tackle criminal activity arising from anti-social behaviour; and
- Covert human intelligence sources such as deployment of undercover officers.

Members were informed that the Authority's current Surveillance Policy was approved by Cabinet in November 2019. The Policy had recently been subject to a review and no amendments (save for minor typographical corrections) had been proposed as the Policy remained fit for purpose.

Regulation and Review Committee were requested to consider the revised draft policy and to recommend the Policy to Cabinet for consideration on 30 November 2020.

The aims of the Authority's policy were to ensure:

- Compliance with RIPA; the relevant Codes of Practice and guidance issued by the Home Office; and guidance from the Investigatory Powers Commissioner's Office (IPCO);
- Give effect to the rights of citizens to respect for their private and family lives; and
- Protect the Authority from legal challenge when undertaking surveillance.

It was noted that the Codes of Practice indicated that, in addition to an annual review of the general surveillance policy, a local authority should consider internal reports on the use of RIPA at least quarterly to ensure that it was being used consistently in compliance with the Authority's policy. It was explained that since 1 November 2012 there had been no authorisations granted and no report other than the annual review to the Committee had been required. Should an authorisation be granted it would be reported to the next available meeting of the Committee to ensure the requirements for elected member oversight of the use of the Authority's RIPA powers had been discharged.

The Committee was informed that organisations using RIPA are subject to regular inspection by the Investigatory Powers Commissioner's Office (IPCO). The Authority received a virtual online inspection visit from the IPCO on 7 September 2020. The purpose of the inspection was to examine the policies, procedures, operations and administration the Authority had in place in relation to the use of directed surveillance and convert human intelligence sources. The outcome of the inspection was very supportive of the Authority's actions to manage its responsibilities under RIPA.

It was **agreed** to note the report and recommend the proposed Policy to Cabinet for adoption.

North Tyneside Council
Report to Regulation and Review Committee
Date: 21 October 2021

Title: Annual Review of Council Policy on Covert Surveillance

Report from Service Area:	**Law and Governance**	
Responsible Officer:	**Bryn Roberts, Head of Law and Governance**	**(Tel: 0191 643 5339)**
Wards affected:	**All**	

PART 1

1.1 Executive Summary:

The Cabinet at its meeting on 29 November 2021 will consider an updated Covert Surveillance Policy. In accordance with the Codes of Practice applying to the Regulation of Investigatory Powers Act 2000 (RIPA) the Authority's Policy is subject to annual review. A copy of the draft Policy for 2022 is attached at Appendix 1. Regulation and Review Committee are requested to consider the revised draft policy and to recommend the Policy to Cabinet for their consideration at their meeting on 29 November 2021.

1.2 Recommendation(s):

It is recommended that the Committee:

1. note the Authority's draft Policy on Covert Surveillance (attached at Appendix 1); and

2. recommend the proposed Policy to Cabinet for adoption at its meeting on 29 November 2021.

1.3 Information:

1.3.1 Introduction

The Authority's current Surveillance Policy was approved by Cabinet in November 2020 and is subject to annual review. The Policy has been subject to a review by Officers and the revised draft policy is attached at Appendix 1. No amendments are proposed (save for minor typographical corrections) to the draft Policy as the previously adopted Policy remains fit for purpose.

The aims of the Authority's Policy are to:

- Set out the Authority's arrangements for complying with RIPA; the relevant Codes of Practice and guidance issued by the Home Office; and guidance from the Investigatory Powers Commissioner's Office (IPCO);
- Give effect to the rights of citizens to respect for their private and family lives (pursuant to the Human Rights Act 1998); and
- Protect the Authority from legal challenge when undertaking surveillance.

1.3.2 The RIPA Shield

The Regulation of Investigatory Powers Act 2000 (RIPA) puts covert surveillance on a statutory basis. RIPA enables certain public authorities, including this Authority, to carry out surveillance operations with statutory protection from legal challenge. It is often referred to as the "RIPA shield".

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

i. the acquisition and disclosure of communications data such as telephone billing information or subscriber details e.g. to tackle rogue traders;
ii. directed surveillance - covert surveillance of individuals in public places e.g. to tackle criminal activity arising from anti-social behaviour; and
iii. covert human intelligence sources (CHIS) such as the deployment of undercover officers.

The RIPA provisions may only be used to authorise surveillance activities in order to detect and prevent serious crime and any authorisation is subject to a requirement to seek authorisation from an 'Authorising Officer' and to obtaining judicial approval from the Magistrates' Court before any surveillance is undertaken. The Authorising Officers within the Authority are:

Paul Hanson – Chief Executive; and
Colin MacDonald – Senior Manager, Technical & Regulatory Services

Officers from Law and Governance accompanied by the relevant Authorising Officer will present any authorisation to the Magistrates' Court for judicial approval. All authorisations will be subject to an internal scrutiny process prior to being submitted for such approval.

Local authorities may undertake surveillance for other purposes, but such surveillance will not benefit from the RIPA shield and will leave a local authority vulnerable to challenge. For this reason, all surveillance activity undertaken by the Authority, whether within the RIPA regime or not, must be appropriately authorised by one of the Authorising Officers and is subject to central monitoring and challenge.

1.3.3 Central Register

The Authority has a Central Register of all RIPA and non-RIPA surveillance activity. The Central Register is maintained and monitored by Law and Governance.

1.3.4 Inspection

Organisations using RIPA are subject to regular inspection by Investigatory Powers Commissioner's Office (IPCO).

The Authority received a virtual online inspection visit from the IPCO on 7 September 2020. The purpose of the IPCO inspection was to examine the policies, procedures, operations and administration the Authority has in place in relation to the use of directed surveillance and covert human intelligence sources.

The outcome of the inspection was very supportive of the Authority's actions to manage its responsibilities under RIPA. A small number of recommendations were made in relation to the information that is provided to Officers in the Covert Surveillance Employee Handbook to update it and provide further clarity. The Employee Handbook is available to Officers, for reference and guidance in relation to the use of RIPA and covert surveillance, on the Authority's internal Intranet webpages. The update of the Handbook to reflect the recommendations is concluded and has been uploaded onto the Intranet. A further recommendation was in relation to training. The inspector recommended that the Authority undertakes as it has in previous years, a training and familiarisation process for Officers who may use covert surveillance as a part of their role. This training will include all members of the Senior Leadership team. The training will be delivered by Officers from Law and Governance who co-ordinate/oversee the use of RIPA and covert surveillance by the Authority. A training module has been developed and will be made available on the Learning Pool. Officers required to undertake the training will be notified in due course.

The Inspector made no recommendations in relation to the Authority's Covert Surveillance Policy and commented that it "is a succinct summary of the approach the Council will take towards the use and management of covert powers".

The Committee are requested to review the draft Policy and recommend to Cabinet that the Policy be adopted.

1.3.5 Summary of Use of Surveillance, Acquisition of Communications Data and CHIS

It should be noted that following the changes to the RIPA regime from 1 November 2012 reported to the Committee in October 2012, there have been no authorisations of any kind granted. The ground most commonly used for authorising covert surveillance addressing anti-social behaviour was removed on 31 October 2012. Authorisations may now only by sought on the grounds that it relates to the prevention and detection of serious crime. Serious crime is defined as crime punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. The latter are all offences involving sale of tobacco and alcohol to underage children.

Law and Governance keeps the Central Record of authorisations under review and advises Authorising Officers/Designated Persons of changes in approach or procedure.

1.3.6 Corporate Responsibilities

The Codes of Practice advise that a Senior Responsible Officer (SRO) should be identified to ensure the Authority has appropriate policies and processes that accord with RIPA and the related Codes of Practice.

The Officer Delegation Scheme places the Senior Responsible Officer role with the Head of Law and Governance.

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.

All employees connected with surveillance and handling of evidence are responsible for ensuring that they act only in accordance with their level of responsibility and training and in accordance with the Policy and associated documents. To assist in this an 'Employee Handbook: Use of Covert Surveillance, Covert Human Intelligence Sources and Communications Data', has been prepared. The Handbook provides key information for Officers and directs them towards key sources of detailed guidance. It is kept under review and revised as necessary to ensure it reflects current procedures and best practice.

If Officers wish to undertake surveillance that falls outside of the RIPA regime they must take legal advice and seek appropriate authorisation. 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 by the Authority.

Use of Social Media for the collection personal information

The application of the requirements of RIPA to the use of informants via, in particular, social media is a developing area of surveillance law. Social Media provides the opportunity for the Authority to monitor, for example, individual rogue traders who trade on-line in the context of trading standards investigations. The continued monitoring of the activities of an individual or the development of a relationship with a trader with the purpose eliciting information from the trader may fall within the RIPA regime.

As stated above this is an area which is continuing to be monitored as it develops, and Officers from Law and Governance and Trading Standards are considering how such activities should actually be undertaken and whether those activities go as far as requiring a RIPA authorisation.

In addition, the Authority may undertake such surveillance for activities that could not benefit from the protection of the RIPA shield i.e. the activity being investigated would not meet the serious crime test, for example, in child protection. Such surveillance may simple be the monitoring of entries on social media (e.g. Facebook) for calling, for example, beach parties or where concerns about breaches of the social media policy may arise. In these circumstances whilst the surveillance is not unlawful it leaves a local authority more vulnerable to challenge as it still entails the collection information about an individual. For this reason, the Authority requires that all surveillance activity undertaken by the Authority outside of the RIPA regime must be appropriately authorised by one of the Authorising Officers and is subject to central monitoring.

Further information has been and will be provided to Heads of Service to raise awareness of RIPA, the circumstances when a RIPA authorisation is necessary and those circumstances where surveillance activity outside of the RIPA regime must still be appropriately authorised. Additionally, a Use of Social Media in Investigations policy is being developed to provide specific guidance in relation to the use of Social Media.

1.3.7 Compliance and Oversight

The Codes of Practice indicate that elected members of a local authority should review its use of RIPA and set the general surveillance policy at least annually. A local authority should also consider internal reports on the use of RIPA at least quarterly to ensure that

it is being used consistently in compliance with the Authority's Policy and that the Policy remains fit for purpose. It has not been possible to give quarterly reports on the use RIPA since 1 November 2012 as no authorisations have been granted. It was agreed by the Committee in 2015 that the use of RIPA should be reported to the Committee on an exception basis. Therefore, when an authorisation is granted, it will be reported the next available meeting of the Committee to ensure the requirements for member oversight of the use of the Authority's RIPA powers are discharged.

To meet these requirements the Policy Statement provides that:

- Cabinet receives an annual report covering the Authority's use of RIPA powers, and review of the Policy for the following year;
- Reports are presented to the Regulation and Review Committee on the Authority's use of RIPA powers. The Committee's role is to look at compliance, oversight and use of RIPA. The Committee will also consider whether the Policy remains fit for purpose and recommend changes to the Policy as appropriate for Cabinet's consideration; and
- The Elected Mayor who has responsibility for RIPA related activities receives regular updates from the Senior Responsible Officer regarding the use of the Authority's powers.

1.3.8 Closed Circuit Television (CCTV) Systems

North Tyneside Council's CCTV control room operates cameras throughout the Borough. Overt surveillance as conducted through the use of CCTV is covered by the Data Protection Act 1998 and not by RIPA. Signage is in place informing the public when they enter zones covered by CCTV equipment. The Council's CCTV control room is registered with the Surveillance Camera on Commissioner under the Data Protection Acts.

If the CCTV cameras are used for covert surveillance (whether by the Authority or the Police), a RIPA authorisation is required. The Police may make formal written requests for surveillance of a target for which they have a RIPA authorisation. The CCTV Control Room Co-ordinator will seek written confirmation of this authorisation.

1.4 Appendices:

Appendix 1: Policy on Covert Surveillance (draft)

1.5 Contact officers:

Wendy Rochester, Information Governance Manager – Information Governance (0191 643 5620)

1.6 Background information:

The following background papers/information have been used in the compilation of this report and are available at the office of the author:

- Regulation of Investigatory Powers Act 2000 and relevant Orders
- Home Office Code of Practice

PART 2 – COMPLIANCE WITH PRINCIPLES OF DECISION MAKING

2.1 Finance and other resources

The provisions of the Policy can be implemented within the Service's existing resources.

2.2 Legal

The Policy has been prepared with reference to the relevant law and Codes of Practice. A number of Statutory Instruments and Codes of Practice published by the Home Office govern the operation of RIPA.

The Authority may only authorise directed surveillance where it is both necessary and proportionate to the investigation or operation being undertaken and to what is being sought to achieve in terms of evidence gathering. Senior Officers are appointed as Authorising Officers and have a key role in carefully scrutinising all applications for the use of RIPA powers under a specific authorisation. Judicial approval is required from the Magistrates' Court in relation to all authorisations prior to any surveillance being undertaken.

Authorising Officers must ensure that authorisations are granted only in appropriate cases and that the extent of all authorisations are clearly set out.

The Authority cannot authorise intrusive surveillance under RIPA. Intrusive surveillance would involve placing an investigator on residential premises or in a private vehicle or allowing the use of an external surveillance device outside of the premises or vehicle that gives the same quality of information as if it was on the premises or in the vehicle.

The Policy, together with the Employee Handbook covers the procedures to be followed in seeking authorisations, maintaining appropriate oversight of the Policy and the central record of decisions.

2.3 Consultation/community engagement

The Policy is aimed at ensuring adherence to the best practice contained within the Codes of Practice as well as the law.

Internal consultation has taken place with Officers with responsibility for the management and supervision of surveillance activity as well as with the Elected Mayor.

2.4 Human rights

Human rights implications are addressed within the report and the Policy. RIPA provides a framework under which surveillance activity can be authorised and conducted in a way that is compatible with the rights of individuals.

The Authority must also ensure that activity that falls outside of the RIPA regime is subject to careful scrutiny and authorisation to ensure that human rights are respected, and the activity is lawfully undertaken.

2.5 Equalities and diversity

There are no equalities and diversity implications directly arising from the report.

2.6 Risk management

The Authority's Policy and the procedures contained in the Employee Handbook are designed to ensure the Authority complies with the law and Codes of Practice and thereby reduce the risks associated with surveillance activity.

2.7 Crime and disorder

RIPA may only be utilised by the Authority for the purposes of detecting and preventing crime.

2.8 Environment and sustainability

There are no environment and sustainability implications directly arising from this report.

This page is intentionally left blank

(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.

This page is intentionally left blank