Telford & Wrekin
Co-operative Council

Protect, care and invest
to create a better borough

Regulation of Investigatory Powers (RIPA)

Corporate Policy & Guidance

February 2023

Abbreviations:

CCTV	Closed Circuit Television
CSP	Communications service provider
Council	Telford & Wrekin Council
CHIS	Covert human intelligence sources
DVLA	Driver and Vehicle Licensing Agency
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedom agreed on 2 November 1950
HRA	Human Rights Act 1998
IPCO	The Investigatory Powers Commissioner's Office
NAFN	The National Anti-Fraud Network
PFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SPOC	Single Points of Contact for acquisition and disclosure of communications data
SRO	Senior Responsible Officer (Chief Executive & Statutory Head of Paid Service)

What RIPA does and does not do

RIPA does:

- Require prior authorisation of directed surveillance
- Prohibit officers from carrying out intrusive surveillance
- Compel disclosure of communications data from telecom and postal services providers
- Permit officers to obtain records from communications service providers
- Require authorisation of the conduct and use of a CHIS
- Require safeguards to be put in place for the use and safety of a CHIS

RIPA does not:

- Make unlawful conduct lawful
- Prejudice or replace any existing power to obtain information/evidence during an investigation. For example information via the DVLA or Land Registry
- Apply to activities outside the scope of Part II of RIPA. The Council can only engage RIPA when in performance of its 'core functions', i.e. the functions specific to the Council as distinct from other public authorities

CONTENTS

1. INTRODUCTION

1.1 The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when public authorities seek to obtain private information about a person by means of surveillance.

1.2 Part II of the Regulation of Investigatory Powers Act 2000 (the 2000 Act) provides a statutory framework under which covert surveillance activity undertaken by the Council can be authorised and conducted compatibly with Article 8 and the UK Data Protection Act 2018/UK GDPR.

1.3 The Information Commissioner's Office - Employment Practices Code provides a framework under which surveillance activity of employees can be authorised and conducted compatibly with Article 8 and the UK Data Protection Act 2018.

1.4 Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

1.5 Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

1.6 Specifically, covert surveillance may be authorised under the 2000 Act if it is either intrusive or directed:

- **Intrusive surveillance** is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device);

- **Directed surveillance** is covert surveillance that is not intrusive but is carried

out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under the 2000 Act).

1.7 The grounds on which local authorities can rely on to authorise directed surveillance are narrower than those available to the police or security services. A local authority can only authorise directed surveillance of a member of the public if the designated person believes such surveillance is necessary and proportionate for the purpose of preventing or detecting crime.

1.8 In most cases the crime for directed surveillance must be an offence for which there is a minimum prison sentence of 6 months, and the surveillance must be authorised by a magistrate.

1.9 The Council must have a policy in place to ensure that such directed surveillance is carried out in compliance with the law and does not breach the human rights of any of the surveillance subjects, and that surveillance in or around the workplace is also carried out in compliance with the law.

1.10 The Protection of Freedoms Act 2012 amended s28 of the 2000 Act and brought in the requirement for a magistrate to approve a RIPA authorisation when the crime threshold was met (criminal offences which attract a minimum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco). Part 2 of the PFA 2012 specifically made changes to surveillance methods including CCTV and ANPR systems.

1.11 The Investigatory Powers Act 2016 (IPA 2016) provided powers to local authorities to access communications data in order to carry out their statutory functions as a Competent Authority under the UK Data Protection Act 2018.

2. POLICY STATEMENT

2.1 Telford & Wrekin Council supports the objectives of the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the Protection of Freedoms Act 2012. This policy aims to assist staff with meeting their statutory and other obligations which includes issues relating to information governance.

3. SCOPE

3.1 The policy applies to all surveillance carried out by the Council, including external surveillance covered by RIPA authorisations, communication data acquisitions covered by the IPA 2016 and internal surveillance covered by the Employment Practices Code.

4. AIM

4.1 To provide a framework for the carrying out of covert surveillance of the public and staff by the Council.

4.2 To ensure all legal obligations on the Council are met, in particular, the Human Rights Act 1998.

5. CONSEQUENCES OF FAILING TO COMPLY WITH THIS POLICY

5.1 Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA and this policy may result in the Council's actions being deemed unlawful by the Courts under Section 6 of the HRA or by the Investigatory Powers Tribunal, opening up the Council to claims for compensation and loss of reputation. Additionally, any information obtained that could be of help in a prosecution will be inadmissible.

5.2 The obligation to comply with RIPA and all related UK and EU information legislation applies to all staff, contractors or others permitted to carry out surveillance on behalf of the Council, who may be held personally accountable for any breaches of Article 8

of the Human Rights Act 1998 (Right to Privacy).

All uses of RIPA should be referred to Legal Services for preliminary advice at the earliest possible opportunity.

6. APPLICABILITY TO INVESTIGATIONS CARRIED OUT BY OR ON BEHALF OF TELFORD & WREKIN COUNCIL

6.1 The majority of the Council's surveillance activity will be overt surveillance i.e. will be carried out openly. For example (i) where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted; or (ii) where the Council advises a tenant that their activities will be monitored as a result of neighbour nuisance allegations or (iii) where an officer uses body worn cameras and informs the individual that the camera will be switched on and recording will take place. This type of overt surveillance is normal Council business and is not regulated by RIPA.

6.2 This policy applies to covert surveillance activities carried out by or on behalf of the Council and includes, but is not limited to, the following:

- the taking of photographs of someone in a public place or;
- the recording by video cameras of someone in a public place;
- the use of listening devices or photographic equipment in respect of activities in a house, provided the equipment is kept outside the house and the equipment gives information of less quality and detail than devices which could have been placed in the house itself
- the taking of photographs of staff in the workplace or;
- the recording by video cameras of staff in the workplace;
- acquisition of communications data e.g. telephone call logs, subscriber details.

7. REVIEW AND MAINTENANCE

7.1 This policy is agreed and distributed for use across the Council by the Director: Policy & Governance on behalf of the Corporate Senior Management Team. It will be reviewed every two years by the Director: Policy & Governance, who will forward any recommendations for change to both Cabinet and the Council for consideration and

approval.

8. LEGAL REQUIREMENTS

8.1 The Council is obliged to comply with all relevant UK and retained EU information legislation. This requirement to comply is devolved to Elected Members, staff, contractors or others permitted to carry out surveillance on behalf of the Council, who may be held personally accountable for any breaches of Article 8 of the Human Rights Act 1998 (Right to Privacy).

8.2 The acquisition of a RIPA authorisation will equip the Council with the legal protection (The RIPA 'Shield') against accusations of a breach of Article 8.

8.3 The Council shall comply with the following legislation and any other legislation as appropriate, including but not limited to:

- The UK Data Protection Act 2018;
- The UK General Data Protection Regulation 2018;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Protection of Freedoms Act 2012;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- The Investigatory Powers Act 2016;

9. OBJECTIVES

9.1 The policy is intended to provide a framework for carrying out surveillance activities in compliance with the law by:

- Creating and maintaining within the organisation an awareness of the Right to Privacy (Article 8, Human Rights Act 1998) as an integral part of the day to day business;
- Ensuring that all staff are aware of and fully comply with the relevant legislation as described in policies and fully understand their own responsibilities when undertaking surveillance activities;
- Ensuring that all staff acquire the appropriate authorisations when undertaking surveillance activities;
- Storing, archiving and disposing of sensitive and confidential surveillance information

in an appropriate manner.

9.2 The Council will achieve this by ensuring that:

- Regulatory and legislative requirements are met;
- RIPA and surveillance training is provided;
- All breaches of privacy, actual or suspected, are reported, investigated and any resulting necessary actions taken;
- Standards, guidance and procedures are produced to support this policy.

10. RESPONSIBILITIES

10.1 The Chief Executive (Statutory Head of Paid Service) is the Senior Responsible Officer for RIPA.

10.2 The Director: Policy and Governance, is the Senior Information Risk Owner and has overall responsibility for information governance within the Council.

10.3 The Director: Policy & Governance is also responsible for:

- Acting as the Council's RIPA Monitoring Officer
- Developing, implementing and maintaining the relevant corporate information governance policies, procedures and standards that underpin the effective and efficient surveillance processes;
- Support and advice to staff and managers on surveillance;
- The production, review and maintenance of surveillance policies and their communication to the whole Council;
- Provision of professional guidance on all matters relating to surveillance;
- Oversight management of all privacy breaches and suspected breach investigations;
- Provision of corporate training;
- Provision, via the Intranet, of surveillance briefing materials and on-line training;
- Management and recording of RIPA authorisations;
- Providing returns to national inspectors e.g. Investigatory Powers Commissioner's office (IPCO)
- Liaising with national inspection regimes, IPCO and the CCTV commissioner to organise inspections;
- Production of an annual Information Governance Report.

10.4 The RIPA Authorising Officers will assess and authorise RIPA applications.

10.5 The Director: Policy & Governance will be made aware of IPA Communications data requests via the National Anti-Fraud Network (NAFN) process.

10.6 The Director: Policy & Governance will authorise all internal intercept requests.

10.7 Where applicable, the Corporate Investigations Team will advise and assist in all aspects of staff investigations and internal intercept requests.

10.8 All Directors will:

- Implement this policy within their business areas;
- Ensure compliance to it by their staff;
- Sign off applications for surveillance of staff;
- Take all reasonable steps to protect the health and safety of investigators and where appropriate of third parties involved with investigations. This should include the carrying out of risk assessments.

10.9 Elected members will review any updated policy, and receive annual reports on surveillance activities via Cabinet.

11. SURVEILLANCE PRINCIPLES

11.1 Telford & Wrekin Council is committed to a surveillance framework that ensures:

- Applications for Authorisations will be made and managed in accordance with the Authorisation Procedures set out at Appendix 2;
- Requests for Authorisations will be assessed to ensure the privacy of the individual is not breached unless it is necessary and proportionate to do so;
- All requests will be monitored, and performance indicators made available to demonstrate compliance with the legislation;
- The surveillance process will be audited by the relevant Service Delivery Managers to ensure compliance with statutory requirements and that relevant national codes of practice are followed.

12. INTRUSIVE SURVEILLANCE

12.1 Intrusive surveillance is covert surveillance carried out by an individual or a surveillance device in relation to anything taking place on residential premises or in any private vehicle. ***The Council is not permitted to carry out intrusive surveillance in any circumstances***.

13. DIRECTED SURVEILLANCE

13.1 Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

13.2 The Council will use Directed Surveillance to acquire information covertly where it is appropriate and legal to do so.

13.3 At the start of an investigation, council officers applying for a RIPA authorisation must satisfy themselves that what they are investigating is a criminal offence and passes the criminal threshold test.

13.4 The appropriate Directed Surveillance application form, which will be available on the Council's intranet site, should be completed and submitted to the Authorising Officer.

13.5 Any officer completing the Directed Surveillance RIPA application form must contact Legal Services to obtain an application reference number and to ensure that they are authorised to attend the magistrate's court on behalf of the Council.

13.6 The applying officer must submit the signed Directed Surveillance RIPA application, once it is signed by the Authorising Officer, to the local Magistrate for approval.

13.7 A higher level of authorisation to apply to the Magistrates Court is required in relation

to RIPA activity where a greater degree of privacy may be expected, or where confidential information might be obtained. For the purposes of RIPA this includes:

- Communications subject to legal privilege;
- Communications between a member of parliament and another person on constituency matters;
- Confidential personal information; and
- Confidential journalistic material.

Due to the confidential nature of such information it is subject to a stringent authorisation procedure and the Directed Surveillance may only be authorised by the Head of Paid Service or their deputy in their absence.

Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from Legal Services prior to making any application.

13.8 The Director: Policy & Governance will ensure there is always a minimum of three (3) trained Authorising Officers at the Council. These will be at Service Delivery Manager level or above, and their names will be published on the Council's intranet.

13.9 Statistical returns for directed surveillance data acquired using RIPA will be submitted to the IPCO by the Director: Policy & Governance upon request.

13.10 The Director: Policy & Governance will comply with requests from the IPCO in relation to the organisation of inspections of the Council.

13.11 A Directed Surveillance RIPA authorisation may also be used if the crime threshold is not met but the offence is a criminal offence under:

(i) sections 146, 147 or 147A of the Licensing Act 2003; or

(ii) section 7 of the Children and Young Persons Act 1933 (underage sales of alcohol and tobacco).

13.12 A RIPA authorisation is not needed when it is not reasonably practicable for an authorisation to be sought for the carrying out of the surveillance in an immediate

response to events.

14. COVERT HUMAN INTELLIGENCE SOURCES

14.1 Under the 2000 Act, a person is a CHIS if:

a) [an officer] establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

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

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

14.2 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

14.3 The Council may use a covert human intelligence source (CHIS) to acquire information covertly where it is appropriate and legal to do so. A CHIS covertly uses a relationship to obtain information or to provide access to any information to another person.

14.4 Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

14.5 However, by virtue of section 26(8) (c) of RIPA, there may be instances where an individual, who covertly discloses information though not tasked to do so may nevertheless be a CHIS. The important question is how did the member of the public acquire the information which they volunteer? If they acquired it in the course of, or as a result of the existence of, a personal or other relationship, they are likely to fall within the definition of a CHIS. If the Council then makes use of the information, and the informant is thereby put at risk, the Council may be in breach of its duty of care owed to the individual. It is recommended that legal advice is sought in any such circumstances.

14.6 The crime threshold does not apply to the authorisation of a CHIS.

14.7 The appropriate CHIS application form, which will be available on the Council's intranet site, should be completed and submitted to the Authorising Officer.

14.8 The applying officer must submit the signed CHIS RIPA application, once it is signed by the Authorising Officer, to the local Magistrate for approval.

14.9 The Council will never authorise the use of a CHIS under the age of 16 to gather evidence against his parents or carers.

14.10 The Council will never authorise the use of a CHIS under the age of 18 unless the protections contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

14.11 If confidential information or matters subject to legal privilege are to be acquired by the CHIS, or the CHIS is a juvenile or a vulnerable individual, the Directed Surveillance may only be authorised by the Head of Paid Service.

14.12 Monitoring of internet and/or social media sites as part of investigations or enforcement activity must be carried out in compliance with the relevant Code of Practice.

15. ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

15.1 From 29 November 2016 the acquisition of communications data was brought under the Investigatory Powers Act 2016. Communications data covers telecommunications operators and postal operators involved in the retention of communications data.

A telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK. A postal operator is a person providing a postal service to a person in the UK.

15.2 The term ‘communications data’ embraces the ‘who’, ‘when’ and ‘where’ of a communication but not the content; not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine external to the Council.

15.3 All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories:

- Entity data – this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices);
- Events data – events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time

Examples of entity data include:

- Who is the subscriber of a phone number
- Who is the account holder of e-mail account
- Who is entitled to post to a web space
- Account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments
- Information about apparatus or devices used by, or made available to, the subscriber or account holder,
- Information about selection of preferential numbers or discount calls.

Examples of events data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records)
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent

that content of a communication, such as the subject line of an e-mail, is not disclosed)

Postal definitions

A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose (or one of its main purposes) is to make available or facilitate the transmission of postal items containing communications. Communications data in relation to a postal service is defined at section 262(3) of the Act and comprises three elements:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted – this includes any information that identifies, or appears to identify, any person or location to or from which a communication is or may be transmitted
- Data relating to the use made by a person of a postal service – this includes the use of services like redirection or the costs that subscribers have paid for delivery
- Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service and which relates to the provision of the service – this includes information about any person to whom a service is provided, whether a subscriber or guest user and whether or not they have ever then used that service

15.4 Applications can be made for entity data (data that associates or links people, identifies people) or event data (data that identifies or describes events) if the criteria set out in s.60A of the Act are met.

15.5 The Council is not able to use IPA to authorise the interception or acquisition of the content of communications, or for access to internet connection records.

15.6 There is a crime threshold for the acquisition of communications data. Entity data can be obtained for the purpose of preventing or detecting crime or of preventing disorder. In order to obtain event data the threshold of “serious crime” as defined in section

86(2A) needs to be met. Officers need to be mindful of this threshold when applying for event data as the offence that they are investigating may satisfy the threshold for entity data but not for event data.

15.7 In accordance with section 73 of the IPA, all local authorities who wish to acquire communications data under the Act must be party to a collaboration agreement. As members of National Anti-Fraud Network (NAFN) the Council use NAFN's shared SPOC services. Applicants within local authorities are therefore required to consult a NAFN SPOC throughout the application process.

15.8 Applications for communication data will be made using the NAFN website. The accredited SPOCs at NAFN will scrutinise the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner.

15.9 Before the application is viewed by the NAFN SPOC, the application will be reviewed by an Authorising Officer within the Council, who will consider the application taking into account the offences under investigation, the proportionality and necessity of the application. They are not authorising the application; they are confirming that they are aware of the application. However, the application cannot proceed with NAFN until the Authorising Officer has agreed the application through the NAFN website.

15.10 There is no requirement for judicial sign off for IPA applications for communications data, as the SPOC at NAFN and the Authorising Officer from the Office of Communications Data Authorisations (OCDA) review the application in detail considering proportionality, necessity and compliance with the Act.

15.11 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

15.12 Any communications data obtained under the IPA application process will be retained in accordance with the Investigatory Powers Act 2016 Codes of Practice. The SPOC from NAFN can provide advice and guidance on the use, storage and retention of data obtained under the Act

15.13 Where a request is refused by an authorising officer from OCDA, the Council has three options:

- Not proceed with the request;
- Resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data
- Resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.

15.14 Statistical returns for communications data acquired using IPA will be submitted to the Investigatory Powers Commissioner by the Director: Policy & Governance upon request.

15.15 The Director: Policy & Governance will comply with requests from the Investigatory Powers Commissioner and the National Anti-Fraud Network (NAFN) in relation to the organisation of inspections of the Council.

15.16 Council staff will refer to the Investigatory Powers Act 2016 Codes of Practice issued by the government and guidance issued by the Council when applying for communications data. The Home Office Investigatory Powers Act 2016 Codes of Practice can be found on the Home Office website.

16. REVIEWS, RENEWALS AND CANCELLATIONS OF RIPA AUTHORISATIONS

16.1 The applying officer must review the authorisation on a monthly basis to decide if the operation needs to continue.

16.2 RIPA authorisations must be cancelled as soon as they are no longer required. Cancellations must be authorised by the Council's Authorising Officer.

16.3 RIPA authorisations are only valid for 3 months. If a renewal is required, it must be applied for prior to the three-month deadline. Renewals must be authorised by the Council's Authorising Officer and the magistrate.

17. REPORTING ERRORS IN RIPA AUTHORISATIONS

17.1 All errors in RIPA authorisations must be reported immediately by the applying officer or Authorising Officer to the Director: Policy & Governance.

18. RIPA REQUESTS FROM THIRD PARTIES

18.1 Requests from third parties to use Council equipment, facilities, CCTV or buildings quoting RIPA authorisations must be made in writing, including a copy of the RIPA authorisation (redacted if necessary) and referred to the Director: Policy & Governance.

19. CCTV

19.1 The Council operates CCTV systems, the use of which is subject to the Surveillance Camera Code of Practice, as amended, as adopted by the Council.

19.2 Where CCTV cameras are used covertly as part of an operation to observe a known individual or group, an appropriate authorisation must be applied for.

19.3 The Council will keep its CCTV protocol up to date.

19.4 The Director: Policy & Governance will comply with requests from the CCTV Commissioner in relation to the organisation of inspections of the Council.

19.5 Any statistical returns required by the CCTV Commissioner will be supplied to him by the Director: Policy & Governance upon request.

20. SURVEILLANCE OF EMPLOYEES AND NON-RIPA SURVEILLANCE

20.1 The Council may use surveillance and the acquisition of internal communications data where there are grounds to do so. Procedures must be followed in relation to its staff where it is appropriate and legal to do so to protect the Council against claims of a breach of Article 8. A RIPA authorisation is not available in these circumstances. It is good practice to apply the same process however to address Article 8 considerations.

20.2 All managers must consider the impact on the human rights of the staff member(s)

under formal surveillance and complete [one of] the appropriate form[s] which can be found on the Council's intranet.

20.3 The Council will follow the ICO's 'Employment Practices Code' to ensure employees' personal information is respected and properly protected under the UK Data Protection Act 2018.

20.4 For the acquisition of communications data (including but not limited to cryptag logs, email accounts, computer access, printing logs, internet use logs and telephone call logs) and internal CCTV footage, managers must complete the 'Interception of Communications Form' which can be found on the Council's intranet and submit it to the Corporate Investigations Team.

20.5 For all other directed surveillance of staff, managers must complete the 'Non-RIPA Surveillance Form' which can be found at Appendix 1 and on the Council's intranet and submit it to the Director: Policy & Governance once it has been signed by the relevant Director.

20.6 RIPA does not grant powers to carry out surveillance. It simply provides a framework that allows the Council to authorise and supervise a defined category of surveillance in a manner that ensures compliance with the Human Rights Act 1998. Equally RIPA does not prevent surveillance from being carried out in other circumstances that fall outside the RIPA framework.

20.7 There may be times when it will be necessary to carry out covert Directed Surveillance or use a CHIS other than by using RIPA. For example, in relation to an investigation into an allegation that a contractor is not carrying out their work as contracted, if a serious disciplinary offence by a member of staff is alleged e.g. gross misconduct, or children are at risk where Court Orders are not being respected, then a RIPA authorisation is not usually available because "criminal proceedings" are not normally contemplated.

20.8 Similarly, there may be serious cases of neighbour nuisance or involving anti-social activity which involve potential criminal offences for which the penalty is below the

thresholds which would enable use of a RIPA authorisation. Nonetheless in such cases there may be strong grounds for carrying out Directed Surveillance or use of a CHIS. Indeed there may be circumstances in which Directed Surveillance or use of CHIS is the only effective means of efficiently obtaining significant information to take an investigation forward.

20.9 Officers should be particularly careful to ensure that individuals who are not a CHIS at the outset of an investigation do not inadvertently become a CHIS by a process of "status drift". If, for example a complainant volunteers to obtain further information about a person being investigated, care should be taken to consider whether the proposed action would involve the complainant becoming a CHIS and if so whether that is appropriate and in accordance with RIPA and the CHIS Code of Practice. Advice should be sought from Legal Services if such conduct is suspected.

20.10 In the circumstances outlined above, a Non-RIPA surveillance application form may be completed in accordance with this Policy. The application must be submitted in the normal fashion to the Authorising Officer who must consider it under the necessity and proportionality test in the same way they would a RIPA application. The normal procedure of timescales, review and cancellations must also be followed.

20.11 The authorisation, regular review, the outcome of any review, renewal applications and eventual cancellation must be carried out in the normal way and using the same timescales as would be applicable to a RIPA investigation. However, for non RIPA surveillance the requirement to seek approval from the Magistrates Court is not relevant. The authorisation for non RIPA surveillance takes effect from the date that it is authorised by the Authorising Officer.

21. SOCIAL MEDIA

21.1 In some investigations, social media sites can form a useful source of intelligence. Usually a review of open source sites will not require authorisation. However, if reviews are carried out in respect of the same individual on a pre-planned or more than one occasion to establish some sort of information or evidence in respect of that individual, this will amount to directed surveillance and authorisation must be obtained.

21.2 If it is necessary and proportionate for the Council to covertly breach privacy controls (e.g. by becoming an account holders "friend" using a false identity) to conduct an investigation, then a directed surveillance authorisation will be required.

21.3 If in engaging with the person the surveillance involves more than merely reading the sites' contents, then an authorisation for the use and conduct of a CHIS will be required.

21.4 Such activities may be monitored by the Council.

22. STORAGE AND DESTRUCTION OF SURVEILLANCE DATA

22.1 The Director: Policy & Governance will store all signed authorisations electronically centrally in a secure manner.

22.2 All electronic copies of the signed authorisations, will be retained for five years and then disposed of securely, unless it is believed that the records could be relevant to pending or future criminal proceedings, where they must be retained for a suitable further period, commensurate to any subsequent review.

23. COMPLIANCE WITH THE LEGISLATION

23.1 The Council recognises the need to make the contents of this Policy known and to ensure compliance by every employee.

23.2 The Director: Policy & Governance will notify relevant staff of changes to RIPA and surveillance legislation, how these changes will affect them, when they will occur and what is needed to stay within the law.

23.3 Elected members will receive an annual RIPA report via Cabinet, and will be notified of any updates to this policy.

23.4 The Council also recognises the need to make their policies known and accessible to the public. This policy will be published on the Council's website.

23.5 RIPA statistics, suitably redacted as to not reveal specific operations, will be published

on the Council's website annually via the open data site.

23.6 Telford & Wrekin Council expects all employees to comply fully with this policy. Disciplinary action may be taken against any Council employee who knowingly breaches any instructions contained in, or following on from, this policy.

24. RECORDS AND DOCUMENTATION

A) Departmental Records

24.1 Applications, renewals, cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation, and destroyed in accordance with the Council's Retention and Disposal Policy. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

24.2 In relation to communications data, records must be held centrally by the SPOC. These records must be available for inspection by the IPCO and retained to allow the Investigatory Powers Tribunal to carry out its functions.

B) Central Record of Authorisations, Renewals, Reviews and Cancellations

24.3 A central record of directed surveillance, CHIS and access to communications data authorisations is maintained by:

Director: Policy & Governance
Darby House
Lawn Central
Telford
TF3 4NT

24.4 The central record is maintained in accordance with the requirements set out in the Home Office codes of practice. In order to keep the central record up to date

authorising officers/designated persons must, in addition to sending through the Home Office application, authorisation form and Magistrates Court order within one week of the authorisation being approved by the Magistrates Court, send notification of every renewal, cancellation and review on the appropriate notification forms.

C) Surveillance products and communications data:

24.5 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

24.6 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

24.7 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use of covert surveillance to facilitate its use in other investigations.

24.8 Material obtained through the use of directed surveillance, CHIS or acquisition of communications data containing personal information will be protected by the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA). In addition to the considerations above, material obtained must be used, stored and destroyed in compliance with any other legal requirements, including confidentiality, and the Council's Data Protection, Information Security and Records Management Policies available on the intranet.

25. TRAINING AND ADVICE, DEPARTMENTAL POLICIES, PROCEDURES AND CODES OF CONDUCT

A) Training & Advice

25.1 The Director: Policy & Governance will arrange regular training on RIPA. All authorising

officers; designated persons and investigating officers should attend at least one session every two years and further sessions as and when required. Training can be arranged on request and requests should be made to Legal Services. In particular training should be requested for new starters within the Council who may be involved in relevant activities.

25.2 The following resources are available on the intranet:

(i) Corporate policy and procedures;
(ii) Home Office codes of practice on covert surveillance and CHIS;
(iii) Home Office code on acquisition and disclosure of communications data;
(iv) Lists of authorising officers and designated persons (posts and names);
(v) RIPA forms for covert surveillance, CHIS and acquisition and disclosure of communications data;
(vi) The corporate CCTV policy;
(vii) Corporate RIPA training;
(viii) Request for designation as an authorising officer or designated person;
(ix) Council notifications of RIPA renewal.

25.3 If officers have any concerns, they should seek advice on RIPA from Legal Services.

B) <u>Departmental policies, procedures and codes of conduct</u>

25.4 Where in practice, departments have any policy, procedures or codes of practice in relation to RIPA that are different from or in addition to this Code, they must immediately seek advice from Legal Services.

26. COMPLAINTS

26.1 Complaints relating to any surveillance matters must be made in writing and addressed to:

Director: Policy & Governance
Darby House
Lawn Central
Telford
TF3 4NT

26.2 If the complainant is still unhappy following the Director: Policy & Governance's response they must be advised to write to:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ.
Tel. 0207 035 3711

27. MONITORING OF AUTHORISATIONS

27.1 The Chief Executive (Statutory Head of Paid Service) is the senior responsible officer in relation to RIPA and is responsible for:

(i) the integrity of the process in place to authorise directed surveillance, the use of CHIS's and the acquisition and disclosure of communications data

(ii) compliance with Part II of RIPA, the relevant Home Office Codes of Practice and this Policy

(iii) engagement with the Commissioner or Inspectors of the IPCO when they conduct inspections, and

(iv) where necessary, overseeing the implementation of any post-inspection plans recommended or approved by a Commissioner

27.2 The Director: Policy & Governance is also required by law to ensure that the Council does not act unlawfully and will undertake audits of files to ensure that RIPA is being complied with and will provide feedback to the authorising officer/designated person where deficiencies in the RIPA process are noted.

27.3 To facilitate the Chief Executive (Statutory Head of Paid Service) role as the Senior Responsible Officer, the Director: Policy & Governance will provide a periodic update on use of RIPA powers by the Council.

27.4 The Director: Policy & Governance will invite members every two (2 no.) years through the Executive to review the Council's RIPA Policy for that period and to recommend any changes to the Council's policy or procedures and will also provide members with

an annual update on use.

27.5 The IPCO has a duty to keep under review the exercise and performance of the Council's use of covert directed surveillance, CHIS, and the exercise and performance of the Council's use of its acquisition and disclosure of communications data powers. The IPCO will periodically inspect the Council and may carry out spot checks unannounced.

28. FURTHER GUIDANCE

a. Further guidance can be found on the Council's web site.

APPENDIX 1

Telford & Wrekin Co-operative Council

Protect, care and invest to create a better borough

BOROUGH OF TELFORD & WREKIN

NON RIPA SURVEILLANCE APPLICATION FORM

BOROUGH OF TELFORD & WREKIN

NON RIPA SURVEILLANCE APPLICATION FORM

Service Area		**Ref. No.**	

Name of Officer	

Contact Details	
Investigation / Operation Name (if applicable)	
Investigating Officer (if person other than above)	

1. DETAILS OF INVESTIGATION
Describe the purpose of the specific operation or investigation e.g. internal disciplinary investigation. Provide details of the investigation and intelligence case to date to include enquiries already undertaken and their result.

2. DETAILS OF SURVEILLANCE
Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, video recording equipment) that may be used.

Explain the information that it is desired to obtain as a result of the directed surveillance.

3. SUBJECT OF SURVEILLANCE
The identities, where known, of those to be subject of the directed surveillance. **Should include where known name, address, D.O.B. or approximate age.** **If persons unknown please provide any description's or other information that may be known.**

4. MISDEMEANOR UNDER INVESTIGATION
Provide details of what offences or malpractice is under investigation, e.g. Gross Misconduct against. Disciplinary Regulations.

5. INTRUSION AND PRIVACY ISSUES
Detail whether *Confidential Information* such as information relating to legal privilege, health, spiritual counselling or other sensitive information is likely to be obtained against any person as a result of the surveillance activity. **Supply details of any *Collateral Intrusion*.** **Why the intrusion is unavoidable.** **Describe precautions you will take to minimise and manage the collateral intrusion.**

6. NECESSITY AND PROPORTIONALITY
Explain why it is necessary to use the covert methods applied for, can the evidence be obtained by less intrusive methods and explain why this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

7. OFFICERS DETAILS			
Name (print)		**Position:**	
Signature		**Date**	

AUTHORISATION SECTION

8. AUTHORISED YES OR NO? (see below)
If rejected detail the reason why. **If authorised state exactly what activity is being authorised by whom and if necessary what equipment they are authorised to use and in what circumstances. This should include any specific instructions such as the management of any images which may be obtained. Cover who, what, where, when and how.**

9. NECESSITY AND PROPORTIONALITY
Explain why you believe the surveillance is necessary and proportionate to what is sought to be achieved by carrying out the covert activity.

10. CONFIDENTIAL INFORMATION
If confidential information is likely to be obtained (see box 5) state how the information will be managed and disposed of. (Seek advice from Legal Team and data controller if required). May require a higher level of authority.

11. REVIEW	
Where appropriate set a review date taking into account all the circumstances. The review date should be no longer than a month to demonstrate that the process is being managed effectively	
Date	**Comments**

12. AUTHORISING OFFICER DETAILS			
Name (Print)		**Position**	
Signature		**Date**	

APPENDIX 2

AUTHORISATION PROCEDURES

1.0 Authorising Officers/Designated Persons for directed surveillance and CHIS

1.1 **Authorising Officers** are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

1.2 **Designated Persons** fulfil a similar role in relation to applications to obtaining communications data, assessing and approving authorisations and notices.

1.3 ***It is the responsibility of Authorising Officers and Designated Persons to ensure that when applying for authorisation the principles of necessity and proportionality are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.***

1.4 Lists of authorising officers and designated persons are available on the Council's intranet. Any requests for amendments to the lists must be **made in writing and** sent to the Director: Policy and Governance.

1.5 Schedule 1 of statutory instrument No. 521 (2010) prescribes the rank or position of authorising officers for the purposes of Section 30(1) of RIPA (covert surveillance and CHIS). Schedule 2 of statutory instrument No. 480 (2010) prescribes the rank or position of designated person for the purposes of Section 25(2) of RIPA (access to communications data). For Local Authorities they prescribe a "Director, Head of Service, Service Manager or equivalent".

1.6 The Director: Policy and Governance designates which officers can be authorising officers or designated persons. Only these officers can authorise directed surveillance, the use of CHIS and acquisition and disclosure of communications data. **All authorisations must follow the procedures set out in the Policy.** Authorising officers/designated persons are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the Director: Policy and Governance.

2.0 Single Point of Contact (SPOC)

2.1 SPOCs are responsible for advising officers within the Council how best to go about obtaining communications data, for liaising with CSPs, and advising whether

applications and notices are lawful. As required under the latest Acquisition and Disclosure of Communications Data Code of Practice, the Council has engaged the National Anti-Fraud Network (NAFN). NAFN's SPOC services relate only to communications data.

3.0 Authorisation of Covert Directed Surveillance, Use of a CHIS and Acquisition and Disclosure of Communications Data.

3.1 RIPA applies to all covert directed surveillance, use of CHIS and acquisition and disclosure of communications data whether by Council employees or external agencies engaged by the Council. Council officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant application form and forward it to the relevant authorising officer. Authorisations or notices in relation to communications data should be referred to NAFN.

4.0 All uses of RIPA should be referred to Legal Services for preliminary advice.

4.1Directed surveillance, use of a CHIS and acquisition and disclosure of communications data can only be authorised if the authorising officer/designated person is satisfied that the activity is:

(a) **in accordance with the law** i.e. it must be in relation to matters that are statutory or administrative functions of the Council. As such the Council is unable to access communications data for disciplinary matters;

(b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and there is a crime threshold for directed surveillance; and

(c) **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct, or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

4.2 Applicant officers should ask the following types of questions to help determine whether the use of RIPA is necessary and proportionate:

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate)
- how the activity to be authorised is expected to bring a benefit to the investigation

- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the ECHR
- what other reasonable methods of obtaining information have been considered and why they have been discounted

4.3 Authorising officers/designated persons should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable.

Particular consideration should be given to collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation.

4.4 Collateral intrusion occurs when an officer undertaking covert surveillance on a subject observes or gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into account by the authorising officer/designated person, particularly when considering the proportionality of the surveillance.

4.5 Particular care must be taken in cases where **confidential information** is involved e.g. matters subject to legal privilege; confidential personal information; confidential journalistic material; confidential medical information; and matters relating to religious leaders and their followers. In cases where it is likely that confidential information will be acquired, officers must specifically refer this to Legal Services for advice.

4.6 The activity must be authorised before it takes place.

4.7 At the time of authorisation the authorising officer/designated person must set a date for review of the authorisation and review it on that date.

4.8 A copy of the draft Home Office application must be forwarded to Legal Services for them to review and comment as necessary. A unique reference number for the application will also be given.

4.9 Once approved by a Magistrate the completed Home Office application and Magistrates Order must be forwarded to Legal Services within one week of the approval as a scanned document. In the case of a section 22(4) RIPA notice requiring disclosure of communications data a copy of the notice must be attached to the

application form. Legal Services will maintain a central register of the Council's RIPA activity.

5. Approval by Magistrates Court

5.1 After an Authorisation for any of the three investigatory activities (Directed Surveillance, CHIS and Communications Data) form has been countersigned by the authorising officer/designated person, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

5.2 The magistrate will have to decide whether the council's application to grant or renew an authorisation to use RIPA should be approved and it will not come into effect unless and until it is approved by the Magistrates Court.

5.3 A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the surveillance techniques (i.e. Directed Surveillance, CHIS and Communications Data) at the same time.

5.4 ***In cases where there is collaborative working with another agency, for example, the Police, as part of a single investigation or operation, only one authorisation from one organisation is required. This should be made by the lead authority of that particular investigation. Duplication of authorisation does not affect the lawfulness of the investigation or operation, but could create an unnecessary administrative burden. Where the Council is not the lead authority in the circumstances, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.***

5.5 It should be noted that only the initial authorisation and any renewal of the authorisation require magistrates' approval.

5.6 There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified but they do need to be authorised by the Director: Policy & Governance to represent the Council in court.

6. The Role of the Magistrates Court

6.1 The role of the Magistrates Court is set out in section 23A RIPA (for communications data) and section 32A RIPA (for directed surveillance and CHIS).

6.2 These sections provide that the authorisation, or in the case of Communications Data, the notice, shall not take effect until the Magistrates Court has made an order approving such authorisation or notice. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate;
- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:
    - arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA;
    - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied;
- The local authority application has been authorised by an authorising officer or designated person (as appropriate);
- The grant of the authorisation or, in the case of communications data, notice was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
    - 25(3) (for communications data),
    - 29(7)(a) (for CHIS),
    - 30(3) (for directed surveillance and CHIS)

7. The procedure for applying for directed surveillance or use of a CHIS is:

- Applicant officer obtains preliminary legal advice from Legal Services if required
- Applicant officer completes an application
- Applicant seeks comments on draft application and unique reference number from Legal Services
- Authorisation is sought from the Authorising Officer
- Applicant officer/legal representative creates court pack and applicant officer proceeds to court
- Applicant officer organises the directed surveillance or use of a CHIS to take place
- Applicant officer sends copy of the Magistrates Court order to Legal Services

8 Additional Requirements for Authorisation of a CHIS

8.1 A CHIS must only be authorised if the following arrangements are in place:

- there is a Council officer with day to day responsibility for dealing with the CHIS **(CHIS handler**) and a senior Council officer with oversight of the use made of the CHIS **(CHIS controller**);
- a risk assessment has been undertaken to take account of the CHIS security and welfare;
- a Council officer is responsible for maintaining a record of the use made of the CHIS;
- any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating; and
- records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS

9 Additional Requirements for Authorisation of Acquisition and Disclosure of Communications Data

9.1 The rules on the granting of authorisations for the acquisition of communications data are slightly different from directed surveillance and CHIS authorisations and involve three roles within the Council. The roles are:

(i) Applicant Officer

(ii) Designated Person

(iii) Single Point of Contact

9.2 Applicant Officer

This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The application form must:

- set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of crime or preventing disorder.

- describe the communications data required i.e. the telephone number, email address, the specific date or period of the data and the type of data required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted.

- explain why the conduct is necessary and proportionate.

- consider and describe any meaningful collateral intrusion. For example, where access is for 'outgoing calls' from a 'home telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it.

9.3 Designated Person

This is the person who considers the application. A designated person's role is the same as an authorising officer's role in relation to directed surveillance and CHIS authorisations. The designated person assesses the necessity for any conduct to obtain communications data taking account of any advice provided by the single point of contact (SPOC). If the designated person believes it is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

9.4 Single Point of Contact (SPOC)

The accredited SPOCs at NAFN scrutinise the applications independently, and provide advice to applicant officers and designated persons ensuring the Council acts in an informed and lawful manner.

9.5 The procedure for applying for acquisition of communications data:

- Applicant obtains preliminary legal advice from Legal Services
- Applicant officer creates an application using the Cycomms Web Viewer on the NAFN website
- SPOC Officer at NAFN triages and accepts the application into the Cyclops system
- SPOC Officer uses Cyclops to update the application details and completes the SPOC report
- Approval is sought from the Designated Person (DP)
- SPOC sends request for Court Pack preparation to Applicant/Legal Representative
- Applicant/legal representative generates court pack using the Web Viewer and applicant proceeds to court
- SPOC receives signed court documents and sends requests to Communications Service Provider (CSP)
- SPOC receives results back from CSP and returns results to Applicant
- Applicant accesses the Web Viewer and downloads results
- Applicant sends copy Magistrates Court order to Legal Services.

9.6 Urgent Authorisations

By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are no longer available.

9.7 Application Forms

Only the RIPA Forms listed below can be used by officers applying for RIPA authorisation.

(a) Directed Surveillance:
Application for Authority for Directed Surveillance
Application for Judicial Approval for Directed Surveillance
Review of Directed Surveillance Authority
Cancellation of Directed Surveillance
Renewal of Directed Surveillance Authority

(b) CHIS
Application for Authority for Conduct and Use of a CHIS
Review of Conduct and Use of a CHIS
Cancellation of Conduct and Use of a CHIS
Renewal of Conduct and Use of a CHIS

(c) Acquisition and Disclosure of Communications Data

Application for a section 22(4) RIPA Notice
Notice under section 22(4) RIPA requiring Communications Data to be obtained and disclosed

9.8 Duration of the Authorisation

Authorisation/notice durations are:

- for covert directed surveillance the authorisation remains valid for 3 months after the date of authorisation
- for a CHIS the authorisation remains valid for 12 months after the date of authorisation (or four months if a juvenile CHIS is used).
- a communications data notice remains valid for a maximum of 1 month.

Authorisations should not be permitted to expire, they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that all authorisations must be reviewed to decide whether to cancel or renew them.

9.9 Review of Authorisations

Authorising officers/designated persons must make arrangements to periodically review any authorised RIPA activity.

Officers carrying out RIPA activity, or external agencies engaged by the Council to carry out RIPA activity, must periodically review it and report back to the authorising officer/designated person if there is any doubt as to whether it should continue.

For Juvenile CHIS's, the Code of Practice stipulates that the authorisation should be reviewed on a monthly basis.

Reviews should be recorded on the appropriate Home Office form.

A copy of the Council's notice of review of an authorisation must be sent to Legal Services within one week of the review to enable the central record on RIPA to be updated.

9.10 Renewal of Authorisations

If the authorising officer/designated person considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the

authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained.

Renewed authorisations will normally be for a period of up to 3 months for covert directed surveillance, 12 months in the case of CHIS, **4 months** in the case of juvenile CHIS and 1 month in the case of a communications data authorisation or notice.

Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation.

Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form. The reasoning for seeking renewal of a communications data authorisation or RIPA notice should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

All renewals will require an order of the Magistrates Court.

A copy of the Council's notice of renewal of an authorisation must be sent to Legal Services within one week of the renewal together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

9.11 Cancellation of Authorisations

The person who granted or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance, CHIS or communications data authorisation or notice no longer meets the criteria for authorisation.

Cancellations must be made on the appropriate Home Office form. In relation to a section 22(4) notice to a CSP, the cancellation must be reported to the CSP by the designated person directly or by the SPOC on that person's behalf.

Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and all welfare matters are addressed*.*

A copy of the Council's notice of cancellation of an authorisation must be sent to the Legal Services within one week of the cancellation to enable the central record on RIPA to be updated.

9.12 What happens if the surveillance has unexpected results?

Those carrying out the covert surveillance should inform the authorising officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

10 Errors

Proper application of the RIPA provisions, and robust technical systems, should reduce the scope for making errors. A senior officer within a public authority is required to undertake a regular review of errors and a written record must be made of each review. For the Council, this will be the Director: Policy & Governance.

An error may be reported if it is a "relevant error". Under section 231(9) of the Investigatory Powers Act 2016, a relevant error is an error by a public authority in complying with any requirements that are imposed on it by an enactment, such as RIPA, which is subject to review by a Judicial Commissioner.

Examples of a relevant error include where surveillance or CHIS activity has taken place without lawful authorisation, and/or without adherence to the safeguards set out within the relevant statutory provisions or the relevant Home Office Codes of Practice.

Where a relevant error has been identified, the Council should notify the Investigatory Powers Commissioner (IPCO) as soon as reasonably practical, and no later than 10 working days (unless otherwise agreed by IPCO). The process for informing IPCO is set out in the relevant Home Office Codes of Practice, which can be found on the intranet.