RIPA POLICY

WEST SUSSEX COUNTY COUNCIL

(March 2020)

1. INTRODUCTION TO THE REGULATION OF INVESTIGATORY POWERS

This policy meets the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA'), The Protection of Freedoms Act 2012 Home Office's Codes of Practice for Directed Surveillance, Covert Human Intelligence Sources and the Acquisition and Disclosure of Communications Data.

The Codes of Practice will be available to the public on request. The Director of Law and Assurance and all Directors with enforcement responsibilities will hold up-to-date copies of the Codes of Practice. The Office of the Surveillance Commissioner's (OSC) Procedures and Guidance 2016 can be found by following this link: https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf.

This policy provides a summary of the legislation and Codes of Practice. If any officer proposes to use RIPA powers for the first time they should refer to the Codes and contact the Director of Law and Assurance for advice in the first instance.

1. Purpose of this Policy

1.1 Surveillance provides a means of preventing crime and disorder. RIPA provides for the regulation of covert investigation by a number of bodies, including local authorities. RIPA regulates a number of investigative procedures, including access to communications data. There are Codes of Practice for the proper exercise of the powers. See this link: https://www.gov.uk/government/collections/ripa-codes.

1.2 County Council officers as part of their duties may carry out activities which fall within the remit of RIPA and are subject to monitoring and oversight by the Investigatory Powers Commissioners Office and the Interception of Communications Commissioner's Office.

1.3 Officers involved in any kind of surveillance in their role should familiarise themselves with this document and the Codes of Practice. Legal advice should be sought before undertaking any activity within the scope of RIPA.

1.4 This policy demonstrates the Council's commitment to carrying out its enforcement powers and investigations in an equitable and transparent manner respecting the human rights of those who may be affected.

1.5 Officers must note that if they fail to follow the requirements of this Policy, the legislation and the Codes of Practice any of the following may occur:

- 1.5.1 The County Council may be liable to claims alleging breaches of an individual's rights under the Human Rights Act 1998;
- 1.5.2 The admissibility of any evidence obtained may be adversely affected;
- 1.5.3 The safety of the member of the public supplying information may be compromised;
- 1.5.4 If there is no authorisation in place, the ability to apply exemption to disclosure under the Public Interest Immunity may be lost;
- 1.5.5 A complaint of maladministration could be made to the Local Government Ombudsman.

Types of regulated activity

1.6 **Covert Directed Surveillance** is undertaken in relation to a specific investigation or operation where the person or persons subject to the surveillance are unaware that it is or may be taking place. The activity is also likely to result in obtaining private information about a person whether or not it is specifically sought for the purpose of the investigation.

1.7 Investigations may require the use of a **Covert Human Intelligence Source**. These may be undercover officers, agents or informants. Such sources may be used to obtain and pass on information about a third party, without their knowledge, as a result of establishing or making use of an existing relationship. This has implications for a person's privacy and is a regulated activity. A Covert Human Intelligence source would be used rarely and only in exceptional circumstances. Collateral intrusion should be kept to a minimum and all applications should include a risk assessment to address this risk.

1.8 RIPA regulates these activities, and the procedure regarding **the acquisition of telecommunications data**, including obtaining telephone subscriber, billing and account information.

1.9 RIPA provides a statutory system of authorisation and monitoring of surveillance activities with which The County Council must comply to ensure that no individual's rights are unnecessarily compromised.

1.10 RIPA introduced the Investigatory Powers Tribunal to investigate human rights complaints. The Investigatory Powers Act 2016 established the Investigatory Powers Commissioners Office and the Interception of Communications Commissioner to inspect public bodies undertaking covert surveillance and the acquisition of communications data.

1.11 Each officer within West Sussex County Council with responsibilities for the conduct of investigations shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that all operations are carried out lawfully and in accordance with this policy.

2. POLICY STATEMENT

2.1 The main aims of the policy are to set out the surveillance practices and procedures to be used across the County Council, to ensure that all officers act within the law and generate and maintain a proper record of activities and authorisations with the aims of reducing the risk of legal challenge and enabling effective enforcement activity.

2.2 The County Council will not undertake any activity defined within RIPA without prior or emergency authorisation from a trained senior officer who is empowered to grant such consents. It is Council policy for any RIPA usage to be considered only as a last resort.

2.3 No Authorising Officer shall authorise the use of surveillance techniques or human intelligence sources unless the activity can be shown to be necessary for the purpose of preventing or detecting crime or of preventing disorder. The lawful use of RIPA powers requires judicial approval and the criminal offence to be prevented or detected by the exercise of the power must be one punishable by a term of at least 6 months' imprisonment.

2.4 Once satisfied that the activity is necessary, the Authorising Officer must then determine whether the activity is proportionate to what is sought to be achieved. The Authorising Officer must be satisfied that there are no other reasonable means of carrying out the investigation or obtaining the desired information. If the information can be obtained by other means the authorisation should not be granted. In determining proportionality and authorisation the issues to consider are set out in paragraphs 2.5-2.11 below.

2.5 Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. Where confidential information is likely to be acquired, authorisation should only be given in exceptional and compelling circumstances.

2.6 When considering applications for the use of a CHIS, an Authorising Officer must be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and consider the level of intrusion likely to be caused to every person who would be affected by the use of a CHIS and any adverse impact on community confidence that might result from such use or from the information obtained.

2.7 Applications for authorisation of directed surveillance and the use of a CHIS except in emergency where the legislation permits, be made in writing on the appropriate forms.

2.8 Intrusive surveillance operations are defined as activities using covert surveillance techniques on residential premises or in any private vehicle which involves the use of a surveillance device or an individual in such a vehicle or on such premises. West Sussex County Council's officers are **NOT** legally entitled to authorise such activities.

2.9 Public bodies are permitted to record telephone conversations where one party consents to the recording and a Directed Surveillance authorisation has been granted. On occasions, officers of the County Council may need to record telephone conversations to secure evidence.

2.10 Intrusive surveillance operations are defined as activities using covert surveillance techniques on residential premises or in any private vehicle, which involves the use of a surveillance device, or an individual, in such a vehicle or on such premises. West Sussex County Council officers are **NOT** legally entitled to authorise these types of operations.

2.11 However public bodies are permitted to record telephone conversations, where one party consents to the recording being made and a Directed Surveillance authorisation has been granted. On occasions, officers of the County Council may need to record telephone conversations to secure evidence.

3. REGULATED ACTIVITIES

Definition of Surveillance

3.1 Surveillance includes:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
- Recording anything monitored, observed or listened to in the course of surveillance;
- Surveillance by or with the assistance of a surveillance device.

3.2 Surveillance includes the interception of postal and telephone communication where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

3.3 Covert Surveillance is surveillance carried out in a manner calculated to ensure that subjects are unaware that it is or may be taking place. Covert Surveillance involves the systematic surveillance of an individual. The everyday functions of law enforcement will not usually involve covert surveillance.

Directed Surveillance

3.4 Directed Surveillance is surveillance which is:-

- covert;
- not intrusive surveillance;
- undertaken for the purpose of a specific investigation or operation;
- undertaken in such a manner that it is likely that private information about an individual is obtained (whether or not that person is specifically targeted for the purposes of the investigation or operation); and
- not carried out by way of an immediate response to events, which would make seeking authorisation under the Act reasonably impracticable.

4. COVERT HUMAN INTELLIGENCE SOURCES ('CHIS')

4.1. The use of informants or undercover officers is referred to as "covert human intelligence sources". It means establishing or maintaining a personal or other relationship with a person for the covert purpose of facilitating the obtaining of information. The Authorising Officer (see 8) must be satisfied that the use of a CHIS is necessary in the circumstances, that the conduct authorised is proportionate to what it seeks to achieve and that arrangements for the overall control and management of the individual are in place.

4.2. A person is a source (CHIS) if:

4.2.1. they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph 3.1 or 3.2.

4.2.2. they covertly use such a relationship to obtain information or to provide access to any information to another person; or

4.2.3. they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

4.3 A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

4.4 A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

4.5 The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source. This covers the use of professional witnesses to obtain information and evidence. The use or conduct of a source to obtain knowledge of matters subject to legal privilege must be subject to the **prior approval of the Surveillance Commissioner**.

4.6 Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS.

4.7 WSCC Trading Standards will not by default seek RIPA authorisation for covert test purchasing operations for age restricted goods. Each operation will need to be looked at to consider whether there is a specific reason for applying RIPA. This might include the formation of a long term customer relationship between an individual and a retailer, operations over a sustained period or the characteristics of particular premises.

4.8 A directed surveillance authorisation will be obtained if recording equipment were to be used, and test purchase volunteer was not a CHIS.

4.9 Trading Standards will not require the use of RIPA directed surveillance authorisation for routine 'shop floor' under age sales test purchases because it is considered

- highly unlikely that private information would be obtained;
- there is little or no risk of collateral intrusion;
- all sales take place in business premises freely accessible to any members of the public;
- the purchasing process only takes a few minutes;
- observation is specifically focused on the sale of the age restricted product to the young person and the actions of the retailer in relation to the purchaser e.g. do they ask the persons age or for ID.

4.10 The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties.

4.11 However, asking a source to obtain information should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is regulated, whether or not that CHIS is asked to do so. It is possible therefore that a person will become engaged in the conduct of a CHIS without being induced, asked or assisting the person to engage in that conduct.

4.12 If the informant is a CHIS, he or she is a person to whom a duty of care is owed. If information provided by a CHIS is to be acted upon, that information must be independently corroborated before taking action. Only the most exceptional circumstances would merit the use of a vulnerable person as a CHIS. A vulnerable individual is a person who may be susceptible to exploitation and who may be in need of support by reason of physical or mental disability, illness or age. Juveniles are people under the age of 18. For both vulnerable and juvenile sources, the Director of Law and Assurance's advice must be obtained when considering authorisation. An authorisation under RIPA will provide lawful authority for the use of a source.

5. COMMUNICATIONS DATA

5.1 It is crucial that the acquisition of communications data is properly authorised. No officer may seek the acquisition of any form of communication data unless he is authorised to do so and the application has been provided to the appointed Single Point of Contact (SPoC). Applications for access to communications data shall be made via the National Anti-Fraud Network (NAFN) and approved by the Office for Communications Data Authorisations (OCDA) in accordance with the Code of Practice.

6. AUTHORISATION

6.1. The list of Authorising Officers is set out in Annex 9. This list will be regularly reviewed and kept up to date by the Director of Law and Assurance. Authorisations for directed surveillance or the use of a CHIS must be obtained using the appropriate application forms. See annexes 3 and 4.

6.2. Authorisations for access to communications data are processed online by the National Anti-Fraud Network ('NAFN'). Applicants will need to log on to NAFN and complete an application form online. The site includes notes for guidance.

6.3. In cases where authorisation leads to confidential information being acquired or a vulnerable adult or juvenile being used as a CHIS, the Chief Executive, or in his/her absence the Director of Law and Assurance, must sign the authorisation.

6.4. Where an authorisation is approved by the Authorising Officer the applicant will then apply to a Justice of the Peace for judicial approval of the authorisation.

7. SOCIAL NETWORKING SITES

Use of Social Media

7.1 The Council recognises that officers may make ad hoc use of social media, and this is a recognised aspect of routine investigations. It is important that officers who do so are aware of their obligations, and make sure that they do not put themselves or the Council at risk of challenge or penalty. Social networking sites mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise. This includes sites such as 'Facebook' and 'LinkedIn'. In using social media for the gathering of evidence:-

7.1.1. Material that is in the public arena (has been published openly) may be accessed and viewed and used as evidence provided this is limited to occasional use;

7.1.2. officers must not 'friend' individuals on social networks as part of work activity unless authorisation has been obtained;

7.1.3. officers should not use their personal accounts to view the social networking accounts of other individuals for work related purposes;

7.1.4. the adoption of a false identity to establish a relationship and exchange information with another person so as to gain access to material to use as evidence constitutes the use of a covert human intelligence source (CHIS) which requires both internal authorisation and the approval of a magistrate's court;

7.1.5. officers should not view an individual's profile on a social networking site excessively and viewing should only be undertaken in order to obtain evidence to inform their investigation;

7.1.6. regular and planned tracking of information of this kind even if published and open constitutes 'directed surveillance' and should only take place if specifically authorised.

7.1.7. further viewing of open profiles on social networking sites to gather or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate;

7.1.8. officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps MUST be taken to ensure its validity.

8. AUTHORISATION PROCEDURE

General

8.1 Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more or relates to the sale or alcohol or tobacco to underage persons.

8.2 Any officer who undertakes investigations on behalf of the Council shall seek provisional authorisation in writing from an Authorising Officer in relation to any directed surveillance or for the conduct and use of any source. Each provisional authorisation then needs to receive judicial approval before being acted upon. Flowcharts which may be of use when considering whether to undertake covert surveillance or the use of CHIS can be found at annexes 1 and 3.

Who can give Provisional Authorisations?

8.3 An Authorising Officer may grant a provisional authorisation, but this authorisation will not take effect until it receives judicial approval (See paragraph 8.19 et seq). Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can only be granted by the Chief Executive, or, in her absence, the Senior Responsible Officer.

8.4 The Council's authorised posts are listed in Annex 9. This appendix will be kept up to date by the Director of Law and Assurance and added to as needs require. If any council manager wishes to add, delete or substitute a post, a request must be referred to the Director of Law and Assurance for consideration as necessary.

8.5 It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations. Training will be given before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training will be kept by the Director of Law and Assurance.

8.6 Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

8.7 Authorising Officers must also ensure that, when sending copies of any forms to the Director of Law and Assurance, the same are sent in sealed envelopes and marked 'Strictly Private and Confidential'. Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

Grounds for Authorisation – the 'necessary & proportionate' test

8.8 An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance. An Authorising Officer shall not grant a provisional authorisation for the carrying out of directed surveillance, or for the use of a source or for the obtaining or disclosing of communications data unless he believes:

- that a provisional authorisation is necessary and
- the provisionally authorised investigation is proportionate to what is sought to be achieved by carrying it out.

8.9 For local authority investigations, provisional authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing or detecting crime.

8.10 Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference or if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe. The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

8.11 Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more or relates to the sale or alcohol or tobacco to underage persons.

8.12 Careful consideration needs to given by authorising officers to all of these points. Such consideration needs to be demonstrated on the authorisation form. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign the form without thinking about their personal and the Council's responsibilities. Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

8.13 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

Collateral Intrusion

8.14 Before provisionally authorising investigative procedures, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. The Authorising Officer must consider whether there is a risk of collateral intrusion into the private life of any person who is not the primary subject of the investigation. In addition to named individuals, the application should include a description of those who might be at risk of collateral intrusion should authorisation be granted. If the risk of collateral intrusion is significant, the Authorising Officer must decide whether a separate authorisation is necessary for those other people.

8.15 If, during the operation, the privacy of individuals not covered by the initial authorisation is unexpectedly interfered with, the Authorising Officer's consideration must be sought to determine whether the initial authorisation needs to be amended and re-authorised or whether a new authorisation is required.

8.16 When considering collateral intrusion and proportionality, the Authorising Officer must balance the intrusiveness of the activity on the target and others against the operational need for the activity. The Authorising Officer should only authorise the activity that is the least intrusive - unnecessary intrusion must be minimised.

8.17 An application for a provisional authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

8.18 Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

Judicial Approval of Provisional Authorisations and Renewals

8.19 The Council is only able to grant a provisional authorisation or renewal to conduct covert surveillance. All provisional authorisations and renewals must be approved by the Magistrates Court before surveillance commences.

8.20 Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) for the use of directed surveillance, acquisition of communications data or for the use of a CHIS will be subject to judicial approval through a Magistrates Court application.

8.21 The Council must apply to the local Magistrates Court for an Order approving the grant or renewal of an authorisation. A template application form and draft Order are included at **Appendix 6** to this policy. In order to obtain judicial approval, the first page of the template form must be completed and submitted along with a copy of the provisional authorisation and any other relevant supporting documents.

8.22 The Council does not need to give notice of the application to the person(s) subject to the application or their legal representatives. If the Magistrates Court refuse to approve the application, it may also make an order quashing the provisional authorisation.

8.23 Magistrates will give approval only if, at the date of the grant of authorisation or renewal of an existing authorisation, they are satisfied that:

- there were reasonable grounds for believing that the use of the measure is reasonable and proportionate and that these grounds still remain;
- the "relevant conditions" were satisfied in relation to the authorisation.

8.24 Relevant conditions are that:

- the relevant person was designated as an Authorising Officer or Designated Person;
- it was reasonable and proportionate to believe that using the proposed measure was necessary and that the relevant conditions have been complied with;
- the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and
- any other conditions provided for by an order made by the Secretary of State were satisfied.

8.25 Judicial approval will also review that the serious crime threshold has been met in relation to the carrying out of directed surveillance. The threshold is that the directed surveillance is for the purpose of preventing or detecting a criminal offence and meets the following conditions:

- that the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment; or

- constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old) or

- constitutes an offence under section 92 Children and Families Act 2014 (sale of nicotine inhaling products to children under 18 years old) or proxy purchasing of tobacco, including nicotine inhaling products, to children under 18 years old under section 91 Children and Families Act 2014.

It is therefore essential that Investigating officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance. If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

Urgency

8.26 Urgent authorisations to bypass the above requirements are not available in relation to directed surveillance or covert human intelligence sources.

Standard Forms

8.27 All authorisations must be in writing. Standard forms for seeking provisional directed surveillance and covert human intelligence source authorisations are provided at annex 2 & 4. The standard form for obtaining judicial approval is provided at annex 6. All authorisations shall be sought using the standard forms as amended from time to time.

9. DURATION OF AUTHORISATIONS

9.1. All records must be kept for at least three years.

9.2. A written authorisation ceases to have effect at the end of the following periods, unless it is renewed:

9.2.1. Directed surveillance – 3 months.

9.2.2. Conduct and use of a CHIS – 12 months.

9.2.3. A notice issued for the production of communication data will remain valid for one month.

10. REVIEWS

10.1. The regular review of authorisations and notices must be undertaken by the relevant authorising officer to assess the need for the surveillance or notice to continue. The results of the review must be recorded on the central record of authorisations.

10.2. Where surveillance provides access to confidential information or involves collateral intrusion particular attention must be given to the need for surveillance in such circumstances.

10.3. In each case, the Authorising Officer must determine how often a review is to take place and this should be as frequently as is considered necessary and practicable.

10.4. See annexes 2, 4, or 5 for location of review forms.

11. RENEWALS

11.1. If at any time an authorisation or notice ceases to have effect and the Authorising Officer considers it necessary for the authorisation or notice to continue for the purposes for which it was given, s/he may renew it, in writing, for a further period of:-

11.1.1. Directed surveillance – 3 months;
11.1.2. CHIS – 12 months;
11.1.3. Access to communications data – 1 month.

11.2. A renewal takes effect at the time at which the previous authorisation ceased to have effect. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation.

11.3. See annexes 2, 4 or 5 for location of renewal forms.

12. CANCELLATIONS

12.1. The Authorising Officer who granted or last renewed the authorisation or notice must cancel it if satisfied that the authorised measure no longer meets the criteria for which it was authorised. When the Authorising Officer is no longer available this duty falls on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer. See annexes 2, 4 or 5 for location of cancellation forms.

12.2 As soon as the decision is taken that an approved measure should be discontinued or its use no longer meets the criteria for which it was authorised, instruction must be given to those involved to stop the activity. The authorisation does not expire when the activity has been carried out or is deemed no longer necessary. It must be either cancelled or renewed. The date and time when such an instruction was given should be recorded in the central register of authorisations and the notification of cancellation, where relevant.

13. RETENTION AND DESTRUCTION OF MATERIAL

13.1 Confidential material must be destroyed as soon as it is no longer needed. It must not be retained or copied unless for a necessary and specified purpose.

14. CENTRAL REGISTER AND MONITORING

14.1. Each Authorising Officer will notify the Director of Law and Assurance of all authorisations and terminations of the regulated activities. The Director of Law and Assurance will keep written records centrally. All such authorisations and terminations will be monitored and reviewed on a regular basis by the Director of Law and Assurance to ensure compliance with current rules and with this policy. Any breaches of this policy, or the Regulations or Codes of Practice will be pursued with the relevant Director and where necessary, referred to the Director of Law and Assurance as Monitoring Officer.

14.2. A copy of all authorisations, renewals and cancellations together with relevant supporting information shall be forwarded to the Director of Law and Assurance within 5 working days of the date of the authorisation, renewal or cancellation.

14.3. **The Director of Law and Assurance shall:**

14.3.1. Keep a register of the documents referred to above;

14.3.2. Monitor the quality of the documents and information received;

14.3.3. Monitor the integrity of the process in place for the management of any CHIS;

14.3.4. Monitor compliance with Part II of RIPA and the Codes;

14.3.5. Oversee the reporting of errors to the relevant oversight Commissioner and the identification of both the cause of errors and the implementation of processes to minimise any repetition;

14.3.6. Engage with the IPCO Inspectors when they conduct their inspections, where applicable, and

14.3.7. Where necessary, oversee the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

15. PLANNED AND DIRECTED USE OF COUNCIL CCTV SYSTEMS

15.1 The Council's CCTV surveillance systems must not be used for directed surveillance without the Director of Law and Assurance confirming to the relevant operational staff that a valid authorisation is in place.

16. CONSEQUENCES OF NON COMPLIANCE

16.1. If authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be lawful for all purposes.

16.2. Where there is unjustifiable interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

16.3. Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

17. TRAINING

17.1. The Senior Responsible Officer will have and maintain written arrangements for holding and updating copies of any Regulations and their relevance in practice and procedures and for training staff responsible for any relevant enforcement activities and the implementation of this policy.

17.2. The Authorising Officers and Single Points of Contact shall be provided with training to ensure awareness of the legislative framework. Single Points of Contact can only be appointed following attendance at a training course accredited by the Home Office and passing a written examination.

18. COMPLAINTS AND REPRESENTATIONS

18.1 The Director of Law and Assurance will be responsible for responding to complaints under RIPA in liaison with the relevant Director and for the management of representations to the Tribunal established under Part IV of RIPA in respect of any referrals relating to the activities of the County Council together with responsibility for liaison with the Office of the Commissioner.

19. DATA PROTECTION

All data will be kept in accordance with the Data Protection principles and the Council's Information Governance policies**.**

March 2020