Appendix 1

Warwick District Council Regulation of Investigatory Powers Act 2000 (RIPA) Policy

1 Introduction

1.1 In carrying out its statutory duties and as part of the Council's responsibilities to protect the public purse, there may be occasion when surveillance or the gathering of information of a covert nature by individual officers may be required. In exercising this function, the Council must ensure that any action is not unlawful under the Human Rights Act 1998 and therefore must meet the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.

1.2 The Investigatory Powers Commission (IPCO) are now responsible for the oversight of RIPA, and undertake regular inspections to ensure compliance with legislation.

1.3 The main purpose of RIPA is to ensure that the relevant investigatory powers are used in accordance with Human Rights and covers both surveillance of members of the public and members of staff.

1.4 Article 8 of the European Convention on Human Rights states:

> *Article 8.1: Everyone has the right to respect for his private and family life, his home and his correspondence. Article 8.2: There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedom of others.*

1.5 This means that in certain circumstances the Council may interfere with a person's rights outlined in Article 8.1 and 8.2 provided the interference is:

- in accordance with the law
- necessary, and
- proportionate

and in order to ensure that the Council does not act unlawfully in carrying out these duties, the requirements under RIPA must be adhered to. The Council must have procedures in place to ensure that any surveillance undertaken is necessary, proportionate and correctly authorised. Surveillance should only be undertaken where there is no reasonable alternative mechanism for obtaining information and the alleged offences carry a minimum sentence of six months' imprisonment or is a statutory exception relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003.

1.6 This policy is applicable to all employees and agents working for the Council and should be read in conjunction with the Regulation of

Investigatory Powers Act 2000 and the Home Office Covert Surveillance and property Interference revised code of practice 2018.

1.7 Although routine patrols, observation at trouble "hotspots", immediate responses to events and overt use of CCTV are excluded from this policy, the Council can still use these techniques as a means to stop offending behaviour.

2 Warwick District Council Procedures

2.1 Training Officers who are required to undertake surveillance in the course of their duties, and officers with delegated powers to authorise such requests, will be required to attend relevant training on a tri-annual basis to ensure that all surveillance requests comply with RIPA requirements and codes of practice. Officers who have not had relevant training should not request or authorise requests for surveillance.

2.2 The RIPA Monitoring Officer will be responsible for arranging training and keeping a log of those who have attended. Anyone who needs to undertake either of these duties but who has not had training should contact the RIPA Monitoring Officer in the first instance to make the necessary arrangements. All investigating officers and those officers who have been allocated specific roles in accordance with RIPA should be fully conversant with the RIPA codes of practice which are can be found at https://www.gov.uk/government/collections/ripa-codes.

2.3 The Council has an Enforcement Group comprising officers involved in enforcement or investigative activities. The Group meets at least quarterly and is used as a channel of communication regarding RIPA matters.

3 Surveillance

3.1 Officers of this Council are not permitted to undertake intrusive surveillance.

3.2 Social Media and Internet Surveillance

3.2.1 Obtaining information via the internet or a social media platform, may be undertaken in order to view or gather information to assist in preventing or detecting crime or other statutory functions and does not necessarily require a RIPA authorisation. However, there are occasions when authorisation is required and is therefore covered by this policy. Further advice and guidance on the use of social media is attached as an appendix to this policy.

3.3 Covert surveillance

3.3.1 Any officer intending to carry out covert surveillance in the course of their duties will explore and consider all alternative methods available in order to obtain the required information before making a request for the authorisation of surveillance. If surveillance appears to be the only option, then this should be discussed with the line manager. The investigating officer will need to provide sufficient information to enable the line manager to consider whether the level of intrusion caused by using

surveillance is proportionate when considering both the crime that it is believed to have been committed and the likely consequences of that crime, and also the effect that the intrusion may have on other affected parties who are not the subject of the investigation. The officer will be required to complete an application to submit for authorisation. All applications for covert surveillance will be made using the recommended OSC forms.

4 Necessity and Proportionality

4.1 Consideration must be given as to whether information can be obtained using another source other than covert surveillance and if it can, what would be the effect of obtaining it using other means. If the information can be obtained using other means, then covert surveillance should not be used.

4.2 Consideration must also be given as to whether the expected outcome is proportionate to the level of intrusion that covert surveillance may cause. This includes any collateral intrusion, that is the risk of intrusion into the privacy of persons other than the individual being investigated. The investigating officer must set out how they intend to minimise this, surveillance will not be proportionate if it is excessive in the circumstances of the case, or could reasonably be obtained using less intrusive methods.

4.3 Necessity and proportionality should be considered at each stage of the process, once an application is made a quality check will be undertaken by the RIPA Monitoring Officer, this will help to ensure that this has been considered carefully. The authorising officer is also required to consider necessity and proportionality as part of the authorisation process.

4.4 In order to protect the health and safety of both the investigating officer and the subject of the surveillance, a risk assessment should be carried out identifying the risks to both individuals.

4.5 Use of a Covert Human Intelligence Source

4.5.1 It is understood that there may be occasion when an officer would deem it necessary to use a CHIS in order to obtain information relevant to their investigation. Using a CHIS requires officers to receive specific training and certain roles would need to be undertaken other than those required for surveillance purposes. We could provide this training however if officers were not exercising these duties regularly it is doubtful that we could guarantee compliance with the law should a CHIS be used. Therefore, any investigations which require the use of a CHIS will only be undertaken after seeking advice and guidance from the legal team at Warwickshire County Council.

5 Authorisations

5.1 Once completed, the application form should be passed to the RIPA Monitoring Officer for quality checking, the Monitoring Officer will consider whether necessity, proportionality and collateral inclusion has been considered and offer further advice if necessary.

5.2 Following a satisfactory quality review of the application, it will be passed to the authorisation officer for approval. The authorisation officer must record the matters that were taken into account in reaching their decision.

5.3 Wherever possible authorisations other than those which involve the use of a CHIS or where confidential information may be obtained, should be passed to Deputy Chief Executive (BH), in exceptional circumstances authorisation can be sought from Deputy Chief Executive (AJ).

5.4 Confidential Information. If there is a risk that through the use of surveillance, confidential information may be acquired then the authorisation should only be considered by a Deputy Chief Executive in the absence of the Chief Executive. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic information and authorisation in these cases should only be granted in exceptional and compelling circumstances.

5.5 Approval by JP All authorisations and renewals are subject to approval by a JP before they can take effect or continue after the end date. Once authorised the applicant should contact the Monitoring Officer so that arrangements for a court hearing can be made. For further guidance please refer to:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

5.6 The applicant should attend the hearing in order to answer any questions the Judge may have in respect of the investigation together with the RIPA Monitoring Officer who is best placed to answer questions on the policy and practise of conducting covert investigations.

5.8 Authorisation for the use of a CHIS will last for 12 months from the date of the authorisation unless it is renewed.

5.9 An authorisation must be cancelled if it is believed that the surveillance no longer meets the criteria upon which it was authorised and the Cancellation of a Directed Surveillance authorisation form should be used for this purpose. The Monitoring Officer will be responsible for checking that the correct process and timescales have been adhered to by the individual officers.

5.10 Copies of all surveillance forms including refusals should be passed to the Monitoring Officer as soon as they are completed. The Monitoring Officer will be responsible for maintaining the central register for requests and ensuring that the correct timescales are maintained.

5.11 Reviewing authorisations All authorisations must reviewed on a regular basis by the authorising officer to assess the continuing need for surveillance and these review periods should be set at the outset. More frequent reviews will be necessary where the surveillance activities involve a high level of intrusion into private life.

5.12 Individuals will be responsible for ensuring that their own applications for surveillance are reviewed and monitored in accordance with the intervals prescribed by legislation and forward copies of the relevant forms to the

Monitoring Officer. An authorisation will last no longer than 3 months unless an application for a renewal has been made before the end of the 3 months has elapsed, the renewal must be approved by the authorising officer.

5.13 A review will be necessary where the level of intrusion increases above what was originally stated or the circumstances change from those stated in the original request and the authorising officer must reconsider the test of proportionality.

5.14 If the original authorisation provided for surveillance of an unidentified individual and the identity of the individual becomes known during the operation, an immediate review will be required to update the authorisation with the details. This will not require completion of a new authorisation.

6 Surveillance not requiring authorisation

6.1 Authorisation is not required if surveillance is required due to an immediate response to an event or in the circumstances it is not reasonably practicable to obtain authorisation and therefore is not directed surveillance.

6.2 General observation activities do not require authorisation whether covert or overt. Such observations frequently form part of the legislative function of public authorities; for example, attending premises to check that no smoking legislation was being adhered to would not need authorisation because this would be part of the general duties of public authorities.

6.3 The use of CCTV cameras does not require authorisation except when used in a covert and pre-planned manner and in this instance please refer to the CCTV protocol for further guidance.

6.4 The use of a recording device by a covert human intelligence source in respect of whom appropriate use or conduct authorisation has been granted.

6.5 Overt or covert recording of an interview with a member of the public where it is made clear that the interview is voluntary and the interviewer is a member of a public authority.

6.6 The recording of excessive noise levels from adjoining premises where the recording device is calibrated only to record excessive noise levels.

7 Interception of Communications

7.1 Interception of communications can only be undertaken by an officer of the Council in the following circumstances:

- In the course of normal business practise. Employees e mails, telephone conversations and internet access can be monitored without RIPA authorisation for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems.

- Interception with the consent of both parties If both parties consent then RIPA authorisation is not required but any such interception should be recorded in an appropriate manner.
- Interception with the consent of one party Such interception will require RIPA authorisation because it falls within the definition of surveillance, however if the interception forms part of a previously authorised request, additional authorisation is not required.
- Interception of communications where neither party is aware that this is taking place is prohibited unless a Warrant has been granted by the Secretary of State.

8 Responsibilities

Senior Responsible Officer – Andrew Jones, Deputy Chief Executive

Authorising Officers – Christopher Elliott, Chief Executive; Bill Hunt, Deputy Chief Executive; and Andrew Jones, Deputy Chief Executive (by exception only).

RIPA Monitoring Officer – Richard Barr, Audit and Risk Manager

9 Definitions

Authorising Officer: A person who is responsible for providing authorisation to an officer to undertake either directed surveillance or the use of a covert human intelligence source in accordance with Section 30 of the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Prescription of Offices, ranks and Positions) Order 2000 SI No 2417. The relevant officers being the Chief Executive and Deputy Chief Executives as set out in the scheme of delegation.

Confidential Personal Information Section 99(1) of the 1997 Act: Personal Information which a person has acquired or created in the course of any trade, business, profession or other occupation, and which he holds in confidence; and communications as a result of which personal information is acquired or created and held in confidence.

Personal Information Section 99(2) of the 1997 Act: Information concerning an individual (living or dead) who can be identified from it and relating to his physical or mental health or to spiritual counselling or assistance given or be given to him.

Surveillance Section 48(2) of RIPA: • Monitoring, observing, listening to persons, their movements, conversations, other activities or communications • Recording anything monitored, observed or listened to in the course of surveillance • Surveillance, by or with, assistance of a surveillance device.

Overt Surveillance: General observations usually made by staff whilst carrying out their duties, includes surveillance where the subject of the surveillance has been notified that such surveillance will be taking place. Overt surveillance does not require authorisation under RIPA.

Covert Surveillance: Section 26(9)(a) of RIPA: If, and only if, carried out in a manner calculated to ensure that persons subject to the surveillance are unaware that it is taking place.

Directed Surveillance: Section 26(2) of RIPA: Covert but not intrusive, and undertaken • For a specific investigation or operation • In a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for the purposes of an investigation); and • Not as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it.

Intrusive Section 26(3) of RIPA: Only if covert and • Carried out in relation to anything taking place on residential premises or in a private vehicle; and • Involves the presence on an individual on the premises or vehicle or is carried out by a surveillance device. Officers from the Council are prohibited from undertaking intrusive surveillance.

Private Information Section 26(10) of RIPA: In relation to a person, includes any information relating to his private or family life.

Covert Human Intelligence Source (CHIS) Section 26(8)(a)-(c) of RIPA: A person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that • Covertly uses such a relationship to obtain information or to provide access to information to another person; or • Covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Conduct and use of a CHIS Section 26(7)(a)(b) of RIPA: • Conduct Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information i.e. the task in hand • Use Actions inducing, asking or assisting a person to act as a CHIS i.e. setting up the CHIS.