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) is 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. Although this training could be provided, in the event of officers not exercising these duties regularly it is doubtful that compliance with the law could guaranteed 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 Council's legal advisors.

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 the Chief Executive. In exceptional circumstances authorisation can be sought from the Deputy Chief Executive.

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 the 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 Justice of the Peace (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 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.

5.7 Authorisation for the use of a CHIS must be given for the maximum duration from the date approved by the JP/Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. Authorisations should not be allowed to simply expire – they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a directed surveillance authorisation will cease to have effect after three months from the date of approval by the Magistrate unless renewed or cancelled. The durations of authorisation for each type of surveillance are detailed below:

- Directed Surveillance - 3 Months
- Covert Human Intelligence Source - 12 Months
- Juvenile Sources - 4 Months

It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

5.8 An authorisation must be cancelled if it is believed that the surveillance no longer meets the criteria upon which it was authorised or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. A 'Cancellation of a Directed Surveillance' authorisation form should be used for this purpose. Where necessary and practicable, the safety and welfare of the CHIS should continue to be considered after the authorisation has been cancelled, and

risk assessments maintained. The authorising officer should satisfy themselves that all welfare matters are addressed and should make appropriate comment in their written commentary. The Monitoring Officer will be responsible for checking that the correct process and timescales have been adhered to by the individual officers.

5.9 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.

5.10 All authorisations must be 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.

5.11 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.

5.12 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.

5.13 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 The following activities do not require authorisation:

a. Surveillance 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.
b. General observation activities 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.
c. The use of CCTV cameras except when used in a covert and pre-planned manner and in this instance please refer to the CCTV protocol for further guidance.
d. The use of a recording device by a covert human intelligence source in respect of whom appropriate use or conduct authorisation has been granted.

e. 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.
f. 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 practice. Employees' emails, 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 Safeguarding and the Use of Surveillance Material

8.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed surveillance or CHIS activity. This material may include private, confidential, or legally privileged information.

8.2 Authorised Purpose

8.2.1 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes (for CHIS activity, this is 5 years and for surveillance activity, this is 3 years). For the purposes of the Code this is defined as follows:

- It is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA in relation to covert surveillance or CHIS activity;
- it is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- it is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- it is necessary for the purposes of legal proceedings; or
- it is necessary for the performance of the functions of any person by or under any enactment.

8.3 Use of Material as Evidence

8.3.1 Material obtained through directed surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

8.3.2 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council must be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

8.3.3 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. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the prosecuting solicitor. They in turn will decide what is disclosed to the defence solicitor.

8.3.4 There is nothing in RIPA which prevents material obtained under directed or intrusive surveillance authorisations from being used to further other investigations.

8.4 Handling and Retention of Material

8.4.1 All material associated and obtained with an application will be subject to the provisions of all data protection legislation and regulations and CPIA Codes of Practice and to any Council Policies with regard to data retention and security. All Officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

8.4.2 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case

8.4.3 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

8.4.4 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

8.4.5 If an appeal against conviction is in progress when the convicted person is released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

8.4.6 Retention beyond these periods must be justified under data protection legislation and regulations. AOs, through the Council's Data Controller, must ensure compliance with the appropriate Data Protection requirements and any relevant internal arrangements produced by the Council relating to the handling and storage of material.

8.5 Dissemination of Information

8.5.1 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

8.5.2 The obligations apply not just to the Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Officer in Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

8.5.3 A record will be maintained justifying any dissemination of material. If in doubt, seek legal advice.

8.6 Storage

8.6.1 Material obtained through covert surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement applies to all those who are responsible for the handling of the material. It will be necessary to ensure that an appropriate security clearance regime is in place to safeguard the material whether held electronically or physically.

8.7 Copying

8.7.1 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

8.7.2 In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained.

8.8 Destruction

8.8.1 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction, and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

9 Errors

9.1 Proper application of the surveillance provisions in the RIPA codes and this Policy should reduce the scope for making errors.

9.2 Relevant Error

9.2.1 An error must be reported if it is a "relevant error". A relevant error is any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA.

9.2.2 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

9.2.3 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and a full report no later than ten working days after the error is discovered. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

9.3 Serious Errors

9.3.1 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's convention rights (within the

meaning of the HRA) is not sufficient by itself for an error to be a serious error.

9.3.2 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

10 Responsibilities

Senior Responsible Officer – Andrew Jones, Deputy Chief Executive

Authorising Officers – Christopher Elliott, Chief Executive and Andrew Jones, Deputy Chief Executive (the latter by exception only).

RIPA Monitoring Officer – Richard Barr, Audit and Risk Manager

11 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 the Deputy Chief Executive 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 during 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.

12 **Complaints**

12.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers, including those covered by this code. Any complaints about the use of powers as described in this code should be directed to the IPT.

12.2 Complaints should be addressed to: The Investigatory Powers Tribunal, PO Box 33220, London, SWIH 9ZQ.