SURVEILLANCE AND COVERT ACTIVITIES POLICY

V3.0 11 March 2019

1. **INTRODUCTION**:

1.1. The Council has statutory duties of investigation and of proper operation. In order to meet its responsibilities, officers will sometimes consider obtaining information without explicitly making clear that an assessment is taking place. Any activity by Council staff or contractors that is designed to obtain information relevant to criminal or civil concerns about a citizen, service user, or employee without the person's knowledge, is a covert activity. On occasions, so as to assist in concluding an enquiry, formal surveillance of a location or a person may also be considered.

1.2. However the Human Rights Act 1998 (HRA) Article 8; provides that everyone has the right to respect for their private and family life, their home and correspondence and this is the key consideration when officers consider obtaining information using a covert activity or surveillance. This right is however subject to an important qualification as Paragraph 2 of Article 8 provides that:

"There shall be no interference by a public authority with the exercise of this right except such as is 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 the rights and freedoms of others."

1.3. In order to provide for covert activities and surveillance to be authorised and conducted compatibly with Article 8 the Regulation of Investigatory Powers Act 2000 (RIPA) and associated Codes of Practice provide a statutory framework, but do not cover every circumstance when it may be appropriate to support a Council function through undertaking a covert activity or surveillance.

1.4. The purpose of this Policy is to direct officers and contractors as to the requirements that must be in place if any covert activity or surveillance is considered to be necessary on behalf of the Council. The product of covert activities undertaken in respect of an individual is described as 'private information'.

2. **ACTIVITIES NOT INCLUDED IN THIS POLICY**:

2.1. An authorisation in accordance with this Policy is not required if the Council has a specific legal basis for conducting covert activities or surveillance, nor does this Policy apply where the proposed action is not likely to result in the obtaining of private information.

Such as when:

2.1.1. Agreement has been sought and obtained from all those to be monitored

2.1.2. Use of properly signed CCTV, ANPR or BWV systems

2.1.3. Recording of excessive noise, or other activities that a person is displaying to the public

2.1.4. General observations obtained in the course of employees undertaking their public work role

2.1.5. The operational use of any statutory powers of entry, or seizure, on behalf of the Council which are available to an employee in a certain job role

2.1.6. Test purchases when there is no intention to record a specific conversation or establish a relationship with the suspected offender
2.1.7. Reviewing recorded information
2.1.8. Obtaining covertly data, objects, artefacts, fauna, or flora, which is not private information.

3. COVERT ACTIVITY OR SURVEILLANCE COVERED BY THIS POLICY:

3.1. There are seven categories of covert activity that the Council can consider deploying to support its functions and each has a process that must be followed in order to make use of the product from that covert activity.
These are:
3.1.1. Serious crime investigation
3.1.2. Investigating the sale of tobacco, or alcohol to underage children
3.1.3. Acquisition of communications data
3.1.4. Monitoring of the use of Council communications equipment / email system
3.1.5. Undertaking covert activities as part of a Council function or service delivery
3.1.6. Monitoring employees' activities
3.1.7. Immediate response to a situation by an employee

4. REQUIREMENTS:

4.1. If it is considered that in order to carry out an assessment, investigation or enforcement responsibility, that there is a need to acquire private information through using covert activities, then the obligations of this Policy must be followed by employees and contractors.

4.2. Undertaking any covert activities or acquiring any personal data without informing the person under observation, are only appropriate when it is in accordance with the powers of the Council, necessary and a proportionate response in the circumstances.

4.3. This Policy provides for processes to be implemented and followed; so as to ensure that the Council has regard to the HRA and to enable the product of covert activities to be used as evidence to support the implementation of Council responsibilities.

5. RESPONSIBILITIES:

5.1. Chief Officers are responsible for ensuring the implementation of relevant processes for authorising and recording covert methods of obtaining private information.

5.2. Council employees and contractors must complete the relevant authorisation or reporting process required by this Policy; so as to demonstrate that using covert means has been in accordance with statutory controls on obtaining private information.

6. PROCESS REQUIRED FOR EACH TYPE OF COVERT ACTIVITY:

6.1. **Serious crime investigation**:

This is in respect of a criminal offence which is sought to be prevented or detected, which is punishable whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment. If the deployment of a covert activity is being considered then the RIPA process must be followed. This includes following the relevant Code of Practice and obtaining confirmation for the proposed covert activity from a Magistrate; before any covert activity or surveillance can proceed.

6.2. **Investigating the sale of tobacco, or alcohol to underage children**:

This is in respect of an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. If the deployment of a covert activity is being considered then the RIPA process; including following the relevant Code of Practice and obtaining confirmation of any proposed covert activity from a Magistrate must be considered before any covert activity can proceed.

6.3. **Acquisition of Communications Data**:

This must be in accordance with Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA) and the relevant Code of Practice must be followed by employees and contractors.

RIPA Section 21(4) defines three categories of communications data, however Local Authorities are not authorised to acquire "traffic data" i.e. information that identifies any person, equipment or location to or from which a communication is or may be transmitted. Nor does the power to acquire communications data extend to obtaining the content of the communication.

6.4. **Monitoring usage of the Council's electronic communications systems**:

This is required to be in accordance with the Lawful Business Practice Regulations and can only be undertaken after an internal authorisation process, (which is the RIPA process excluding authorisation by a Magistrate) that includes an impact assessment undertaken in line with guidance from the Information Commissioner on the implementation of the DPA.

6.5. **Undertaking covert activities as part of a Council function or service delivery**:

Should an officer consider that undertaking a covert activity or surveillance is necessary in order to progress an assessment or investigation as part of their work role and the activity does not fall under any of the other types of covert activity listed in this policy; then the internal assessment process must be followed, (which is the RIPA process excluding authorisation by a Magistrate).

6.6. **Monitoring employees' activities**:

The observation and monitoring of employees without their knowledge or consent must only be undertaken after an internal authorisation process, (which is the RIPA process excluding authorisation by a Magistrate) that includes an impact assessment, undertaken in line with guidance from the Information Commissioner on the implementation of the DPA.

6.7. **Immediate response to a situation by an employee**:

If because of an employees work role, a person or situation of interest to the Council is suddenly observed, but there is insufficient time to seek a formal authorisation to undertake a covert activity or surveillance in response to immediate events.
An employee can determine that it is appropriate in the light of any known risks to their safety to immediately undertake a covert activity in order to gain private information which seems likely to support the functions of the Council. However the following must then be completed:

6.7.1. Only undertake necessary covert activities or surveillance
6.7.2. Record the events as soon as practicable within the case file
6.7.3. A manager is to review the situation within one working day
6.7.4. The case plan to be updated to identify when and how the person who has been observed is to be told of the information observed or collected
6.7.5. A manager must consider whether authorisation should be considered for any additional covert activity or surveillance.

7. MONITORING AND REPORTING ON THE EXTENT OF COVERT ACTIVITIES:

7.1. Monitoring of the use of covert activities and surveillance is through a report to Councillors by the Senior Responsible Officer (SRO), which is a required role to oversee compliance with RIPA.

7.2. The SRO is the Corporate Director / Chief Information Officer, who must advise the lead Councillor quarterly and report annually to Council on the use of covert activities and surveillance.

7.3. Reports from the SRO are to include analysis of the covert activities undertaken by service teams and the annual returns required by the RIPA oversight Commissioners; so as to enable Councillors to approve activities as being consistent with this Policy.

8. APPROVAL

V3.0 at Audit Committee 11 March 2019

APPENDIX – GLOSSARY AND REFERENCE

Term	Meaning
2000 Act RIPA	Regulation of Investigatory Powers Act 2000. http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatorypowers/
ANPR	Automatic Number Plate Recognition
Authorisation	An application which has received the approval of an authorising officer
Authorising officer	A person within a public authority who is entitled to grant authorisations. List available in Document Library
BWV	Body Warn Video – camera and sound recorder attached to an officer to record interactions with citizens
CCTV	Closed Circuit Television Recording
Code of Practice	Codes of Practice issued under RIPA section 71.
Covert	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. As defined in section 26(9)(a) of the 2000 Act
Lawful Business Practice Regulations	The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provide that it is lawful to intercept a communication with the express consent of the system controller in a number of circumstances. It is lawful for a public authority to monitor staff emails without their consent in order to establish the existence of facts relevant to the business or activities of the organisation. The system controller must make all reasonable efforts to inform staff that their communications may be intercepted. It is permissible to monitor (but not record) communications without individuals' consent to determine whether or not the communications in question relate to the business or activities of the organisation.
Local Authority use of RIPA	Updated from 01/11/2012 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/localauthority-ripa-guidance/
Private information	Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person's personal or family affairs. Private information includes information about any person, not just the subject(s) of an investigation. May include personal data, such as names, telephone numbers and address details.
Surveillance	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. See section 48(2) of the 2000 Act.