HUNTINGDONSHIRE DISTRICT COUNCIL
COVERT INVESTIGATION POLICY
ON THE ACQUISITION OF COMMUNICATIONS DATA,
USE OF COVERT SURVEILLANCE
AND COVERT HUMAN INTELLIGENCE SOURCES

(REGULATION OF INVESTIGATORY POWERS ACT 2000 & INVESTIGATORY POWERS ACT 2016)

Version History

Version number	Date	Author	Reason for New Version
0.1	02/2025	ITS/PB	Update to format and legislative references

Policy Statement

Officers and employees of (and contractors working on behalf of) Huntingdonshire District Council may, in the course of their investigatory, regulatory and enforcement duties, need to make observations of persons in a covert manner, to use a Covert Human Intelligence Source or to acquire Communications Data. These techniques may be needed whether the subject of the investigation is a member of the public, the owner of a business or a Council employee.

By its very nature, this sort of action is potentially intrusive and so it is extremely important that there is a very strict control on what is appropriate and that, where such action is needed, it is properly regulated in order to comply with Legislation and to protect the individual's rights of privacy.

Privacy is a right, but in any democratic society, it is not an absolute right. The right to a private and family life, as set out in the European Convention on Human Rights, must be balanced with the right of other citizens to live safely and freely, which is the most basic function that every citizen looks to the state to perform.

Drawing on the principles set out in the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the Data Protection Act 1998, this policy sets out the Council's approach to Covert Surveillance, the use of Covert Human Intelligence Sources and the acquisition of Communications Data.

The policy also sets out Members' oversight of this area, adopts a set of procedures and appoints appropriate officers to ensure that these areas are properly controlled and regulated.

1. Policy

1.1 All Covert Surveillance, the use of a Covert Human Intelligence Source (CHIS) also known as an informant, and the acquisition of Communications Data by those working for or on behalf of this Council (investigators) will be carried out in accordance with this policy and the associated procedure (the Covert Investigation Procedure).

1.2 Any officer or employee who deliberately or recklessly breaches this policy may be considered to have committed an act of gross misconduct and in those circumstances would be subject to the relevant disciplinary procedures. Elected Members are bound by a Code of Conduct and as such any breaches of this policy may lead to further investigation under this Code.

1.3 In so far as the Regulation of Investigatory Powers Act (RIPA) allows, Covert Surveillance and the use of a CHIS will always be subject to the RIPA application process. This does NOT affect monitoring activities where the actions undertaken do not amount to covert surveillance. Where officers wish to undertake covert surveillance or use informants but where RIPA is not applicable, a similar process of considering the proportionality and necessity of any such activities must be carried out before the activities are undertaken and approval gained from a RIPA authorising officer. When gathering information online, officers are instructed to consider at what point their actions go beyond the scope of open-source enquiries and meet the criteria for covert investigations. In these instances it will be necessary to obtain the relevant RIPA authorisations.

1.4 When acquiring Communications Data, officers are instructed to use the process set out in the Investigatory Powers Act (IPA) and the associated Communications Data Code of Practice, unless they are doing so with the consent of the data subject. DPA requests and other powers may NOT be used to seek the disclosure of Communications Data. Communications data may only be obtained using IPA powers for the applicable crime purpose. It should be noted that the guidance in the statutory code of practice takes precedence over any contrary content of a public authority's internal advice or guidance.

2. Appointments

2.1 The Chief Executive of Huntingdonshire District Council is the *Senior Responsible Officer (SRO)* for RIPA purposes.

2.2 The Corporate Fraud Manager is the *RIPA Co-Ordinator (RC),* who will monitor the use of covert techniques within the Council (whether using the RIPA or non-RIPA processes) and report to members on the activities the policy covers.

2.3 Only those appointed by this policy as Authorising Officers (AOs) may authorise covert surveillance, the use of informants and approve applications for the acquisition of communications data.

2.4 Service Managers and Team Leaders who meet the training criteria will be designated as AOs, subject to a maximum number of six at any given time. The RC will maintain a list of all these designations as part of the RIPA / IPA Procedures.

2.5 The RC will appoint such persons as they may from time to time see fit to be *Single Points of Contact* (SPOC) (or to make such other arrangements as they deem appropriate) for the purposes of acquiring communications data using RIPA.

2.6 In order for the Council's RIPA authorisations to take effect, they must be approved by a Magistrate. All those who may need to apply to a Magistrate to appear for that purpose for the Council must be authorised to do so by the Head of Shared Legal Practice. The RC will maintain a list of all these designations as part of the RIPA Procedures.

3. Oversight and Reporting

3.1 The RC shall report to the Corporate Governance Committee on the use of RIPA and IPA regulated activity by officers of the Council annually. The report must not contain any information that identifies specific persons or operations but must be clear about the nature of the operations carried out and the product obtained.

3.2 Alongside this report, the RC / SRO will report details of any 'Non-RIPA' surveillance undertaken or informants used in precisely the same fashion.

3.3 Elected Members shall have oversight of the Council's policy which will be reviewed annually, unless changes are required sooner.

3.4 The role of Elected Members in this process is to, with reference to the update reports, satisfy themselves that the Council's policy is robust and that it is being followed by all officers involved in this area. Although it is elected members who are accountable to the public for council actions, it is essential that there should be no possibility of political interference in law enforcement operations.

4. RIPA / IPA Procedures

4.1 The RC will create a set of procedures that provide instruction and guidance for the use of surveillance and informants, and the acquisition of communications data ensuring that they continue to be both lawful and examples of best practice.

4.2 The reference to 'maintain and update' in this section includes the duty to remove AOs from the list if they cease to be employed in a relevant role or if they no longer satisfy the requirements to be an AO, and the right to add names to that list so long as they satisfy the policy and regulatory requirements.

4.3 If a change is required in order to comply with this part, the RC is authorised to make that change without prior approval from any person, however the RC must report any changes made under this section to members during the annual oversight of the policy.

4.4 Relevant managers are required to ensure that their staff understand that covert investigation techniques may only be used in accordance with this policy and the associated procedures.

5. Training

5.1 In accordance with this Code of Practice, AOs **must** receive full training in the use of their powers. They must be assessed at the end of the training, to ensure competence, and must undertake refresher training at least every two years. Training will be arranged by the RC. Designated officers who do not meet the required standard, or who exceed the training intervals, are prohibited from authorising applications until they have met the requirements of this paragraph. AOs must have an awareness of appropriate investigative techniques, Data Protection and Human Rights Legislation.

5.2 Those officers who carry out surveillance work must be adequately trained prior to any surveillance being undertaken. Appropriate training will be undertaken to ensure that AOs and staff conducting relevant investigations are fully aware of the legislative framework.

6. Exceptions, Notes and Complaints

6.1 CCTV cameras operated by the Council are not covered by this policy, unless they are used in a way that constitutes covert surveillance; only under those circumstances must the provisions of this policy and the RIPA Procedures be followed.

6.2 Interception of communications, if it is done as part of normal business practice, does not fall into the definition of acquisition of communications data. This includes but is not limited to opening of post for distribution, logging of telephone calls for the purpose of cost allocation, reimbursement, benchmarking, logging emails and internet access for non-work use.

6.3 Complaints regarding the application of this policy can be made via the Council's Complaints Procedure. However, the detail of an operation, or indeed its existence, must not be disclosed as part of a complaint investigation. This does not mean that the complaint will not be investigated, but rather that the result of any investigation would be entirely confidential and not disclosed to the complainant.

7. Duty to Comply

7.1 All those mentioned in this policy are reminded that deliberately or recklessly failing to comply with this policy (or to follow the procedures and processes created in accordance with this policy) may amount to misconduct and could result in disciplinary action. .

Note: The procedures issued under point 4 are confidential and must not be shared outside the council. For more information, please contact the Corporate Fraud Manager