www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

POLICY

ON THE ACQUISITION OF COMMUNICATIONS DATA,
AND USE OF COVERT SURVEILLANCE
AND COVERT HUMAN INTELLIGENCE SOURCES
("COVERT INVESTIGATION POLICY")

Approved by the Audit & Governance Committee on 16 February 2021

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

POLICY

ON THE ACQUISITION OF COMMUNICATIONS DATA, AND USE OF COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

(REGULATION OF INVESTIGATORY POWERS ACT 2000)

Statement

Officers and employees of (and contractors working on behalf of) the Royal Borough of Windsor and Maidenhead 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 and the Data Protection Act 2018, this policy sets out the Royal Borough'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.

Policy

1.1 It is the policy of The Royal Borough of Windsor and Maidenhead (the Council) that all Covert Surveillance, the use of Covert Human Intelligence Sources (informants) and the acquisition of Communications Data (CD) 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). Any member, officer or employee who deliberately or recklessly breaches this policy will normally be considered to have committed an act of gross misconduct and will be dealt with accordingly.

1.2 In so far as the Regulation of Investigatory Powers Act allows, Covert Surveillance and the use of Covert Human Intelligence Sources (informants) will always be subject to the Regulation of Investigation Powers Act (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 available, 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. Officers are instructed to consider when online investigations, where actions go beyond the scope of open source enquiries, would meet the criteria for covert investigations and to obtain relevant authorisations in those cases.

1.3 When acquiring CD 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. Data Protection Act (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. (Note that the guidance in the statutory code of practice takes precedence over any contrary content of a public authority's internal advice or guidance.)

i. The Council resolves to maintain membership of the National Anti-Fraud Network, so that the relevant sections of the IPA and the associated Communications Data Code of Practice may be complied with.

Appointments

1.4 The Council appoints the Managing Director as the *Senior Authorising Officer (SAO)* for RIPA purposes ; it appoints the Council's *Monitoring Officer* as Senior Responsible Officer (SRO) for all purposes under RIPA and IPA.

1.5 The Council appoints the *Lead Specialist (Shared Audit and Investigation Service with Wokingham Borough Council) as the RIPA Monitoring Officer (RMO)* to monitor the use of covert techniques within this Council (whether using the RIPA or non-RIPA processes) and reports to members on the activities the policy covers. They are also directed to ensure that appropriate training is made available to RIPA Authorising Officers (AOs), IPA Verifying Officers (VOs) and applicants when it is required.

1.6 The Council directs that only those appointed by this policy as AOs and VOs may authorise covert surveillance, the use of informants or the acquisition of communications data. In so far as is practical and possible, the council intends that the same officers should be nominated as both AOs and VOs.

1.7 The Council appoints Directors and Heads of Service who meet the training criteria as AOs, subject to a maximum number of six (including the SAO) at any given time. Those appointed as AOs are also appointed to the role of VO if they hold a post of director or above. The Council instructs the RMO to maintain a list of all those currently authorised as part of the Covert Investigation Procedure.

1.8 The Council directs the RMO to 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 by the use of IPA.

1.9 In order for the Council's RIPA authorisations to take effect, they must be approved by a Magistrate. The chief legal officer (Head of Law) is instructed to authorise all those who may need to apply to a Magistrate to appear for that purpose for the Council. The RMO is directed to maintain a list, as part of the Covert Investigation Procedure, of all those so authorised.

1.10 The Council appoints Directors and Heads of Service who meet the training criteria as VOs, subject to a maximum number of six at any given time. The Council instructs the RMO to maintain a list of all those currently authorised as part of the Covert Investigation Procedure.

Oversight and Reporting

1.11 The RMO shall report to elected Members on the use of RIPA & IPA regulated activity by officers of the Council every six months. Such a report shall be presented to the Members (or to such a sub-committee as the full council shall deem appropriate to constitute for oversight purposes) by the RMO and the SRO. 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.

1.12 Alongside this report, the RMO and SRO will report details of 'Non-RIPA' surveillance undertaken or informants used in precisely the same fashion.

1.13 Elected Members shall have oversight of the Council's policy and shall review that policy annually should it be deemed by the RMO that significant changes have been made. At that review (or following any six-monthly report) elected Members shall make such amendments as they deem necessary to the Council's policy, and may give such directions as they deem necessary to the RMO and SRO in order to ensure that the Council's policy is followed.

1.14 Elected Members shall not interfere in individual authorisations. Their function is to, with reference to the 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.**

Covert Investigation Procedure

1.15 The RMO is instructed to create a set of procedures that provide instruction and guidance for the use of surveillance and informants, and the acquisition of communications data. They are further instructed to maintain and update these procedures, ensuring that they continue to be both lawful and examples of best practice.

1.16 The reference to 'maintain and update' in this section includes the duty to remove AOs / VOs 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 / VO, and the right to add names to that list so long as (a) they satisfy the policy and regulatory requirements and (b) at no time does the number of AOs exceed six.

1.17 If a change is required, in the opinion of the RMO, in order to comply with this part, they are authorised to make that change without prior approval from any person.

1.18 The RMO must report any changes made under this section to Members when they undertake their annual oversight of the Policy, as set out above.

1.19 All 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.

Training

1.20 In accordance with this Code of Practice, AOs / VOs **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 RMO. 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 and VOs must have an awareness of appropriate investigative techniques, Data Protection and Human Rights Legislation.

1.21 Those officers who actually carry out surveillance work must be adequately trained prior to any surveillance being undertaken. A corporate training programme has been developed to ensure that AOs, VOs and staff undertaking relevant investigations are fully aware of the legislative framework.

1.22 The Corporate *Leadership Team* members who have no direct involvement with covert investigation will undertake a briefing at least biannually, to ensure that they have a good understanding of the activities that might fall into the definition of covert investigation techniques.

Exceptions, Notes and Complaints

1.23 CCTV cameras operated by this 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 Covert Investigation Procedures be followed.

1.24 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, etc.; logging E Mails and internet access for the purpose of private reimbursement.)

1.25 If any person wishes to make a complaint about anything to which this policy applies is invited to use the Council's Complaints Procedure. Any complaint received will be treated as serious and investigated in line with this Council's policy on complaints. **Regardless of this, the detail of an operation, or indeed its existence, must never be admitted to as part of a complaint. This does not mean it will not be investigated, just that the result of any investigation would be entirely confidential and not disclosed to the complainant.**

Adoption and Amendment of the Policy

1.26 This version of the Policy was approved by the Audit & Governance Committee on behalf of the Council on 16 February 2021 after which it came into immediate effect. It replaces all previous policies on these subjects.

Duty to Comply

1.27 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) will normally amount to misconduct, which can have serious disciplinary consequences, including summary dismissal.

Note: The procedures issued under para 1.15 *et seq* may be found on Share Point.