Report for: ACTION

Contains Confidential or Exempt Information	NO - Part I
Title	Resubmission of Regulatory of Investigatory Powers Act Policy
Responsible Officer(s)	Richard Bunn, Interim Head of Finance
Contact officer, job title and phone number	Catherine Hickman, Service Manager – Shared Audit and Investigation Service, 07917 265742
Member reporting	Cllr Paul Brimacombe
For Consideration By	Audit and Performance Review Panel
Date to be Considered	28 June 2016
Implementation Date if Not Called In	Immediately
Affected Wards	All

REPORT SUMMARY

This report presents the Regulatory of Investigatory Powers Act Policy which aids the Panel to discharge their responsibilities as stated in its Terms of Reference.

If recommendations are adopted, how will residents benefit?	
Benefits to residents and reasons why they will benefit	Dates by which residents can expect to notice a difference
Anti-fraud and anti-corruption work undertaken by the council is supported by robust policies and procedures thereby protecting both the interests of the residents and the council.	Immediately

1. DETAILS OF RECOMMENDATION

RECOMMENDATION: That Audit and Performance Review Panel consider and approve the Regulation of Investigatory Powers Act Policy.

2. REASON FOR RECOMMENDATION(S) AND OPTIONS CONSIDERED

Background

2.1 Article 8 (Right to Respect for Private and Family Life) of the Human Rights Act 1998 (HRA) states that every person shall have the right to respect for their private and family life, home, and correspondence. The Article states that there shall be no interference with this right by any public body except in accordance with the law. The Article, unlike many of the other Articles, does not give an absolute right to privacy where national legislation, compliant with HRA, states that the right can be suspended.

2.2 The Regulation of Investigatory Powers Act 2000 (RIPA) was introduced to provide law enforcement agencies with a legal gateway and strict guidance on when and how the subject of an investigation can have their Article 8 rights suspended. Contrary to much press publicity, local councils can use the powers conferred by RIPA but only for the purposes of the detection and prevention of crime.

2.3 Local councils can use RIPA Authorisations to conduct 'Covert Directed Surveillance' or acquire 'Communications Data'. The Legislation, guidance and Code of Practice for both these areas is provided by the Home Office.

2.4 The Royal Borough of Windsor and Maidenhead (the 'Council') has had policies and procedural guidance in place since 2003, which ensure that officers conducting these activities are fully trained and conversant with both the law and the most recent guidance from the Home Office.

2.5 In October 2012, the Government introduced a stricter regime for Local Authorities when using the provisions of RIPA. The Protection of Freedoms Act 2012 was introduced and restrictions imposed by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, both of which came into force on 1 November 2012. This included the requirement for all applications to be authorised by a Justice of the Peace (JP) and that all RIPA activity, as defined in the Home Office Guidance, to only take place where 'serious crime' was being investigated.

2.6 In early 2013, the Home Office produced new guidance and Codes of Practice for the amended requirements that Local Authorities are required to meet.

Commissioners

2.7 RIPA provided for the creation of two commissioners to oversee the two areas of surveillance which affect the Council. The Office of the Surveillance Commissioner (OSC) and the Interception of Communication Commissioner Office (IOCCO) carry out these two separate functions.

2.8 The Council is required, whether there is a policy in place or not, to provide an annual report to both commissioners on all activity undertaken. The OSC inspect every local council affected by RIPA periodically and the IOCCO conduct random inspections.

2.9 This report presents the Policy and Procedure, which is attached at Appendix A and will be made available on hyperwave.

Option	Comments
Approve the policy and procedure. **Recommended**	This will ensure that activity undertaken on behalf of the council, complies with legislation.
Amend the policy and procedure.	May result in legal challenge through not complying with legislation or inefficiencies for the Council.
Not approve the policy and procedure.	May result in legal challenge through not complying with legislation or inefficiencies for the Council.

3. KEY IMPLICATIONS

Defined Outcomes	Unmet	Met	Exceeded	Significantly Exceeded	Date they should be delivered by
Residents have confidence that public funds are being used economically, efficiently and effectively and that Council assets and interests are being safeguarded from misappropriation / loss.	Significant financial losses to the Council. Loss of residents confidence. Council reputation may be affected.	Financial losses are identified and recovered. Gain residents confidence. Council reputation protected.	N/A	N/A	31 March 2017

4. FINANCIAL DETAILS

Financial impact on the budget

There are no financial implications.

	2015/16	2016/17	2017/18
	Revenue £'000	Revenue £'000	Revenue £'000
Addition	£0	£0	£0
Reduction	£0	£0	£0

	2015/16	2016/17	2017/18
	Capital £'000	Capital £'000	Capital £'000
Addition	£0	£0	£0
Reduction	£0	£0	£0

5. LEGAL IMPLICATIONS

5.1 Relevant legislation includes the Regulation of Investigatory Powers Act (RIPA) 2000

6. VALUE FOR MONEY

6.1 Investigation work is planned to assist the Council in ensuring that its assets are used efficiently and effectively and that they are being properly safeguarded against misappropriation, loss and fraud.

7. SUSTAINABILITY IMPACT APPRAISAL

7.1 N/A

8. RISK MANAGEMENT

Risks	Uncontrolled Risk	Controls	Controlled Risk
1. Failure to have and follow appropriate fraud policies leads to breach of legislation resulting in fines, investigation and reputation damage.	High	Appropriate fraud policies are in place, have been approved and are followed.	Low
2. Failure to provide an investigation service leads to major event, fraud and/or mismanagement of monies.	High	An appropriate investigations service is in place.	Low
3. Failure to have an investigation service in place to investigate potential losses.	High	An appropriate investigations service is in place.	Low

9. LINKS TO STRATEGIC OBJECTIVES

9.1 Helps the Council accomplish its objectives by undertaking investigations into misappropriation, loss or fraud.

10. EQUALITIES, HUMAN RIGHTS AND COMMUNITY COHESION

10.1 N/A

11. STAFFING/WORKFORCE AND ACCOMMODATION IMPLICATIONS

11.1 N/A

12. PROPERTY AND ASSETS

12.1 N/A

13. ANY OTHER IMPLICATIONS

13.1 N/A

14. CONSULTATION

14.1 Consultation has taken place with the Corporate Management Team and S151 Officer.

15. TIMETABLE FOR IMPLEMENTATION

Date	Details
29/06/16	Policy will be implemented with immediate effect.

16. APPENDIX

Appendix A - Regulation of Investigatory Powers Act Policy

17. BACKGROUND INFORMATION

17.1 Previous versions of the above mentioned policy.

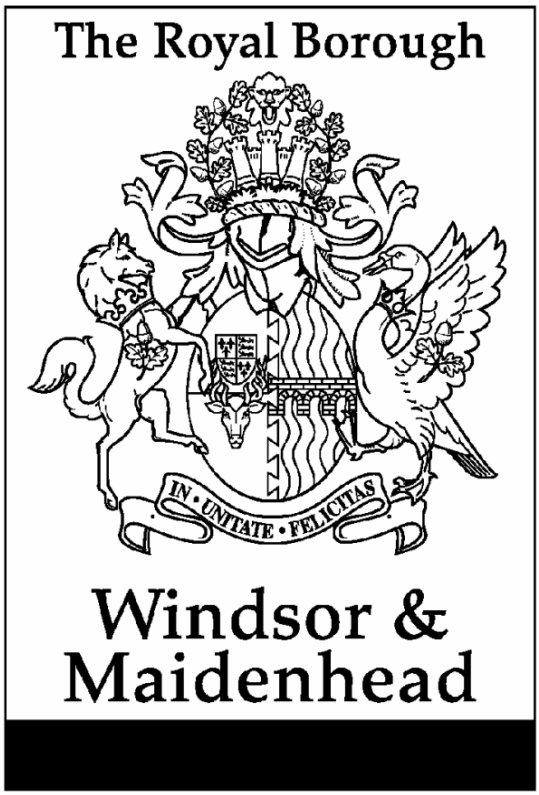
18. CONSULTATION (MANDATORY)

Name of consultee	Post held and Department	Date sent	Date received	See comments in paragraph:
Internal				
Corporate Management Team (CMT)	Managing Director, All Strategic Directors, Head of Finance	02/06/16	09/06/16	MD - Updates to Policy approved.
Legal Services				
Human Resources				
Cllr Brimacombe	Chair of the Audit and Performance Panel			

REPORT HISTORY

Decision type:	Urgency item?
Non-key decision	No

Full name of report author	Job title	Full contact no:
Catherine Hickman	Service Manager, Shared Audit and Investigation Service	07917 265742



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)

Approved by Audit and Performance Review Panel (28 June 2016)

Takes Effect – Immediately after Approval

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 1998, 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 Authority) that all Covert Surveillance, the use of Covert Human Intelligence Sources (informants) and the acquisition of Communications Data by those working for or on behalf of this Authority (investigators) will be carried out in accordance with this policy and the associated procedure. (the RIPA 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 (RIPA) allows, Covert Surveillance and the use of Covert Human Intelligence Sources (informants) 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 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.

1.3 When acquiring Communications Data officers are instructed to use the RIPA process if it is available to them, unless they have a statutory power which allows access to such data (in which case either route may be used).

Appointments

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

1.5 The Council appoints the Service Manager, Shared Audit and Investigation Service as the *RIPA Monitoring Officer* (RMO) and direct that they monitor the use of RIPA within this Council and reports to members on the activities the policy covers. They are also directed to ensure that appropriate training is made available to *Authorising Officers (AOs)* when it is required.

1.6 The Council directs that only those appointed by this policy as AOs may authorise covert surveillance, the use of informants or the acquisition of communications data.

1.7 The Council appoints Directors, Assistant Head of Service and Service Manager levels or equivalent, who also meet the training criteria as AOs, subject to a maximum number of six (including the *SAO*). The Council instructs the RMO to maintain a list of all those currently authorised as part of the RIPA Procedures.

1.8 The Council directs the SAO to appoint such persons as he may from time to time see fit to be *Single Points of Contact* (SPOC) (or to make such other arrangements as he deems appropriate) for the purposes of acquiring communications data by the use of RIPA.

1.9 In order for the Council's RIPA authorisations to take effect, they must be approved by a Magistrate. The RMO is directed to maintain a list, as part of the RIPA Procedures, of all those so authorised.

Oversight and Reporting

1.10 The RMO shall report to elected Members on the use of RIPA 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.

1.11 Alongside this report, the RMO and SRO will report details of 'Non-RIPA' surveillance in precisely the same fashion.

1.12 Elected Members shall have oversight of the Council's policy and shall review that policy annually. 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.

1.13 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.**

RIPA Procedures

1.14 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 the RIPA Procedures, ensuring that they continue to be both lawful and examples of best practice.

1.15 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 (a) they satisfy the policy and regulatory requirements and (b) at no time does the number of AOs exceed six.

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

1.17 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.

Training

1.18 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 RMO. Designated AOs 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.

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

Exceptions, Notes and Complaints

1.20 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 RIPA Procedures be followed.

1.21 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.)

1.22 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

1.23 This version of the Policy was approved by the Audit and Performance Review Panel on behalf of the Council on 28 June 2016, after which it came into immediate effect. It replaces all previous policies on these subjects.

Note: The procedures issued under para 1.14 may be found on hyperwave.