Appendix 1

CITY OF WOLVERHAMPTON COUNCIL

Covert Investigations Policy

Regulation of Investigatory Powers Act 2000

Investigatory Powers Act 2016

wolverhampton.gov.uk

Approved by:	Cabinet 19/06/2013
Published	19/06/2013 V4
Reviewed	12/02/2014 V4.1
Reviewed	19/03/2015 V4.2
Reviewed	01/06/2016 V4.3
Reviewed	01/04/2018 V4.3.1
Reviewed	09/01/2019 V4.4
Amended	25/02/2019 V4.5
Reviewed and Updated	21/01/2021 V4.6

Amendment Sheet

Date	Amendment Number	Amendment	Made by	Authorised by
14/01/2014	1	Addition of amendment sheet and subsequent amendments to index page numbers	SAW	SRO Nick Edwards 12/02/2014
14/01/2014	2	Item 2.2 Political oversight role to be discharged by Cabinet Member – City Services not Cabinet (Resources) Panel as of 11/09/2013	SAW	SRO Nick Edwards 12/02/2014
14/01/2014	3	Addition of Item 3.5 Management of non RIPA surveillance activities	SAW	SRO Nick Edwards 12/02/2014
14/01/2014	4	Correction of Appendix 3 Standards RIPA documentation version status	SAW	SRO Nick Edwards 12/02/2014
14/01/2014	5	Amendment to template WCCRIPA 2000(MCA): clarification of note 1 p2 and addition of 'reference number' p3	SAW	SRO Nick Edwards 12/02/2014
30/01/2015	6	Item 2.9 Replace reference to Cabinet (Resources) Panel with Cabinet Member City Services	SAW	SRO Kevin O'Keefe 19/03/2015
30/01/2015	7	Amended reference to BRDO Age Restricted Products and Services: A Code of Practice for Regulatory Delivery	SAW	SRO Kevin O'Keefe 19/03/2015
30/01/2015	8	Amendment to Authorising Officers, Senior Responsible Officer and SPoC.	SAW	SRO Kevin O'Keefe 19/03/2015
30/01/2015	9	Titles of Council Officers amended to reflect organisational changes eg. Chief Executive replaced with Managing Director, etc.	SAW	SRO Kevin O'Keefe 19/03/2015

Date	Amendment Number	Amendment	Made by	Authorised by
30/01/2015	10	Reference made to Councils Social Media in Investigations policy. Para 3.6	SAW	SRO Kevin O'Keefe 19/03/2015
30/01/2015	11	Amendments to reflect use of NAFN for Communications Data applications.	SAW	SRO Kevin O'Keefe 19/03/2015
30/01/2015	12	Amended references to Codes of Practice and OSC guidance and procedures document	SAW	SRO Kevin O'Keefe 19/03/2015
30/01/2015	13	Amendment to Appendix 3, reflecting changes to template documents for Communications	SAW	SRO Kevin O'Keefe 19/03/2015
01/06/2016	14	p11: Addition of 3.7 relating to Wolverhampton Homes and ASB team	SAW	SRO Kevin O'Keefe 01/06/2016
01/06/2016	15	Para 1.2: Amended definition of intrusive surveillance	SAW	SRO Kevin O'Keefe 01/06/2016
01/06/2016	16	Para 1.2: Amended definition of CHIS	SAW	SRO Kevin O'Keefe 01/06/2016
01/06/2016	17	Para 2.4.1: removal of reference to prevention of disorder	SAW	SRO Kevin O'Keefe 01/06/2016
01/06/2016	18	Para 3.3.2 Role of handler and controller separated	SAW	SRO Kevin O'Keefe 01/06/2016
01/06/2016	19	CHIS Review form title and content corrected	SAW	SRO Kevin O'Keefe 01/06/2016
01/06/2016	20	Changed all references to City of Wolverhampton Council and changed logo	SAW	SRO Kevin O'Keefe 01/06/2016
01/04/2018	21	Authorising Officers removed A.Jervis and S.Martin Amended job titles	SAW	SRO Kevin O'Keefe 01/04/2018
08/11/2018	22	Amendment to Head of Paid Service and addition of Authorising Officer C Howell	SAW	SRO Kevin O'Keefe 08/11/2018
09/01/2019	23	Review of policy and amendments following introduction of new Codes of Practice	SAW	SRO Kevin O'Keefe 09/01/2019
25/02/2019	24	Para 3.4 of Operating Procedure amended authorisation period for juvenile CHIS	SAW	SRO Kevin O'Keefe 25/02/2019
21/01/2021	25	Corporate Policy reviewed and updated	SAW	SRO David Pattison

Date	Amendment Number	Amendment	Made by	Authorised by

Index

A1: Corporate Policy Statement

The City Council is fully committed to operating its covert investigation activities in accordance with the Regulation of Investigatory Powers Act 2000, and the Investigatory Powers Act 2016. The legislation provides protection for the legitimate rights of citizens living or working in the City or visiting Wolverhampton. Whilst fully supporting these fundamental rights, the City Council will deliver effective enforcement services which protect the wider public interest by necessary and proportionate use of lawful covert investigation techniques.

A2: Political Endorsement

Political endorsement for the Policy has been given by Elected Member Forums:
Cabinet: 08/09/10
Sustainable Communities Scrutiny Panel: 12/10/10
Cabinet (Resources Panel): 02/11/10
Cabinet: 19/06/13

A3: Legislative Background

The Regulation of Investigatory Powers Act 2000 was introduced to provide a comprehensive and coherent framework within which public authority enforcement services could undertake covert investigations lawfully. The 2000 Act provides a regime within which enforcement services may undertake covert activities which infringe some of the 'qualified rights', such as the right to privacy, granted to individuals via the Human Rights Act 1998 (HRA). Infringement of such rights is only lawful where public authorities can show that it is necessary to protect the public interest and the level of infringement is proportionate to the public interest issue concerned. Compliance with the Regulation of Investigatory Powers Act and Investigatory Powers Act 2016 is designed to ensure that investigatory actions are HRA compliant.

Information obtained about individuals under the 2000 Act is subject to the controls and safeguards provided by the Data Protection Act 2018 in relation to the acquisition, processing and distribution of personal data. The 2018 Act provides exceptions to the non-disclosure of personal data where it is necessary for the investigation of criminal activities and such data should only be disclosed to organisations outside the Council in accordance with the 2018 Act and the Criminal Procedure & Investigations Act 1996.

The Investigatory Powers Act 2016 governs the use of powers that provide for the lawful acquisition of communications data.

Any monitoring of employees working activities by managers to ensure compliance with the Council's legal, financial and personnel procedures generally falls outside the 2000 Act. The Council as a telecommunications system provider is permitted under specific legislation to monitor use of telephone, email and Internet access systems provided to employees for use in transacting the Council's business.

1.0 Investigatory Practices

1.1 Regulation of Investigatory Powers Act 2000 - Directed Surveillance & Covert Human Intelligence Sources:

Directed Surveillance:

Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under the 2000 Act);

Local Authorities **may** lawfully undertake covert surveillance that is directed at a particular target and may obtain private information about an individual or a business.

Intrusive Surveillance:

Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device).

The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained.

City of Wolverhampton Council CANNOT undertake intrusive surveillance.

Covert Human Intelligence Sources (CHIS):

A person is a CHIS under 2000 Act if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph 26(8) b) or c);

(b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or

(c) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

These may be Council officers or third parties acting under an officer's direction (tasked)

1.2 Investigatory Powers Act 2016 - Access to Communications Data

In accordance with section 73 of the Act, all local authorities wishing to acquire communications data under the Act must be party to a collaboration agreement. City of Wolverhampton Council is a member of the National Anti-Fraud Network and use NAFN's shared SPoC services.

All Communications Data held by a telecommunications operator, or obtainable from a telecommunication system, falls into two categories:

- **Entity Data:** This data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones, tablets and other communications devices).
- **Events Data:** Identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

Applicants are required to process all applications via NAFN and consult with NAFN SPoC officers throughout the application process. The accredited NAFN SPoCs will scrutinise applications independently and all applications submitted will require the approval of the local authority Approved Rank Officer. NAFN will provide advice to ensure the local authority acts in an informed and lawful manner.

Approval of authorisations is carried out by the Office for Communications Data Authorisations.

Section 11 of the 2016 act creates an offence for anyone within a public authority to knowingly or recklessly obtain communications data unlawfully.

2.0 Corporate Policy

2.1 Senior Responsible Officer (SRO)

The Chief Operating Officer to the City Council will act as the Council's Senior Responsible Officer and will be responsible for ensuring that the Council has procedures in place and operating effectively to ensure that the Council complies with its obligations under RIPA and IPA.

2.2 Senior Responsible Officer responsibilities

The Senior Responsible Officer shall be responsible for ensuring that the Council delivers the following functions under RIPA:

Inspections: Responding to requests for information from the Investigatory Powers Commissioners Office (IPCO). Implementing recommendations arising from inspection visits in a timely manner.

RIPA Management Arrangements: Maintaining an effective Central Record of authorisations and ensuring the integrity of RIPA management activities by compliance with the Act and Codes of Practice. Overseeing an Audit Plan to ensure activities are conducted and recorded in a consistent and timely manner across the authority utilising the Corporate Operating Procedure. Promoting RIPA awareness and compliance across all Council services.

RIPA Authorising Officers: Advising the Chief Executive on the appointment of RIPA Authorising Officers and ensuring they are of an appropriate standard. Ensuring that appropriate initial and update training is provided for all officers involved in RIPA regulated activities.

Political Oversight: To ensure effective delivery of the political oversight and involve Elected Members in an annual review of the corporate policy and a quarterly consideration, where necessary, of how effectively Council services have complied with the Policy in delivering RIPA regulated activities. This role will be discharged by the Cabinet Member Governance and the Governance and Ethics Committee.

The Senior Responsible Officer shall be responsible for ensuring that the Council delivers the following functions under IPA:

Integrity of the process in place within the public authority to acquire communications data

Compliance with Part 3 of the Act and with the relevant code of practice, including responsibility for novel or contentious cases

Oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors

Quality Assurance of applications submitted to OCDA by the public authority

Engagement with the IPC's inspectors when they conduct their inspections; and where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

2.3 RIPA Management in Directorates

Directors shall ensure that RIPA regulated activities are delivered by their officers in accordance with the Corporate Policy implementing the 2000 Act, relevant Home Office Codes of Practice and good practice guidance issued by the Home Office or Commissioners Office.

2.4 Authorising Officers

Authorising Officers for RIPA must satisfy the minimum rank requirements of Director, Head of Service, Service Manager or equivalent. The Senior Responsible Officer will ensure that a sufficient number of appropriately trained officers are appointed to act as Authorising Officers.

Where Confidential Information, including legally privileged information, is likely to be acquired or where a CHIS aged under 18 is to be authorised the authorisation must come from the Head of Paid Service (Chief Executive).

Confidential Information is defined in the Codes of Practice as details of a person's medical history, spiritual counselling or material subject to journalistic or Parliamentary privilege.

The principal duty of Authorising Officers is to ensure that the authorisation requested is necessary to address the issue concerned and that the level of intrusion is proportionate when balanced against the public interest in addressing the issue. Authorising Officers should not be directly involved in the activities that they are authorising. **Appendix 1** details the Council's RIPA and IPA prescribed officers.

2.5 Corporate Operating Procedure

All Authorising Officers and Applicants shall have regard to the Councils Corporate Operating Procedure which details the procedures to be used in **Appendix 2**.

2.6 Standard RIPA Forms

All RIPA activity must be authorised in writing by an Authorising Officer, using Standard Forms, any amendments to standard form templates must be approved by the Senior Responsible Officer. All standard forms are contained in **Appendix 3**.

2.7 Approval by the Magistrates Courts and the Office for Communications Data Authorisations

The Protection of Freedoms Act 2012 introduced a requirement that Directed Surveillance and CHIS authorisations cannot be implemented until the Authorising Officer's decision has been approved by an order issued by the Magistrates Court.

In addition, the renewal of an Authorisation also requires approval by the Court, the Court will consider what reviews have been undertaken in order to determine if the Authorisation should be renewed. The Authorising Officer will attend Court to obtain the order and will be delegated to make the application on behalf of City of Wolverhampton Council, under Section 223 of the Local Government Act 1972.

All applications for Communications Data are processed via NAFN, with notification being made to the 'Made Aware' officer, as detailed in Appendix 1. The decision to approve or reject lies with the Office for Communications Data Authorisations.

2.8 Corporate Control of RIPA Regulated Activities

A RIPA Co-ordinator shall be appointed and shall exercise effective oversight and quality control of the Central Record. They will be responsible directly to the Senior Responsible Officer. The RIPA Co-ordinator will identify when reviews, renewals and cancellations of authorisations are due and will ensure that the Corporate Central Record of Authorisations is updated promptly.

The RIPA Co-ordinator will be responsible for the issue of a sequential Unique Reference Number for each Authorisation. This shall be obtained by the Applicant from the RIPA Co-ordinator prior to an application being made to an Authorising Officer.

2.9 Corporate Central Record

The Home Office Codes of Practice require that each public authority have a single centrally retrievable record, known as the Central Record of Authorisations to provide an overview of its RIPA activities and assist the Commissioners in carrying out their duties of oversight when visiting the authority.

The Central Record is maintained by the RIPA Co-ordinator under the control of the Senior Responsible Officer. The content is generated by the prompt submission of original Authorisation, Review, Renewal and Cancellation documentation to the RIPA Co-ordinator.

All Services undertaking RIPA regulated activities must ensure that original forms are forwarded to the RIPA Co-ordinator, any copies retained should be held in a secure manner.

The Senior Responsible Officer will provide the Cabinet Member Governance with a Quarterly Report on Authorisations and a commentary on compliance with the Corporate Policy. An annual reports and review of this policy will be presented to the Governance and Ethics Committee.

The Council will retain records for a period of at least five years from the ending of an Authorisation.

2.10 Engagement with Commissioners

The Commissioners make periodic requests for information and undertake inspection visits to public authorities and the Council's response to such contacts will be managed by the Senior Responsible Officer.

2.11 Error Reporting

Errors in delivering RIPA activities are defined in the relevant Codes of Practice and shall be reported promptly to the Senior Responsible Officer. The Senior Responsible Officer shall ensure oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.

Errors shall be notified to IPCO on the Error report Form, see **Appendix 4**.

3.0 Operational Considerations

3.1 Limits on Use of Directed Surveillance

Authorising Officers may **not** grant an authorisation for the carrying out of Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and it meets additional conditions, namely that the offence under investigation is punishable on summary or indictment by a maximum term of at least 6 months of imprisonment or would constitute an offence under S146, S147 and S147A of the Licensing Act 2003 (namely the sale of alcohol to children, allowing the sale of alcohol to children and persistently selling alcohol to children) or S7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under 18).

3.2 Management of Directed Surveillance & CHIS Authorisations

The Corporate Operating Procedure provides common requirements for the management of Directed Surveillance and CHIS Authorisations including the process for Application, Review, Renewal and Cancellation of Authorisations and the requirement to undertake a CHIS risk assessment.

3.3 Management of Communications Data Access

Access to Communications Data from Communication Service Providers can only be undertaken by NAFN SPoC Officers who are registered with the Home Office. The Head of Audit acts as the' Made Aware' officer and is listed in Appendix 1.

Local Authorities may only access entity and event data and **cannot** engage in interception of communications ie the content of Postal, Telephone or Email communications.

3.4 Management of surveillance of employee activity

Surveillance of employee's for compliance with Council procedures relating to time recording or use of Telephone, Email and Internet systems fall outside of RIPA and this Policy. They are governed by officer's terms of employment and HR rules.

Clearly any surveillance of officers suspected of conduct amounting to a disciplinary breach should be based on considerations of necessity and proportionality. Monitoring of the use made of Telephone, Email and Internet systems provided by the Council for business use by employees is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These regulations allow the Council to monitor the usage of the Council's telecommunications systems by employees including the interception of the content of communications. This power is essential to ensure that the Council complies with its legal and contractual obligations to employees to avoid harassment at work and its financial obligations to ensure that employees do not use publicly funded facilities for personal use or gain.

3.5 Management of Covert Surveillance which does not meet the criminal threshold

Where covert surveillance is considered, which does not meet the criminal threshold under the Regulation of Investigatory Powers Act. Officers shall have regard to the Human Right Act 1998 and comply with the Councils Policy and Procedure for Surveillance under the Human Rights Act. See **Appendix 5**

3.6 Management of Overt Surveillance activity

Where overt surveillance is undertaken which is clearly outside the remit of RIPA, officers shall have regard to the Home Office Surveillance Camera Code of Practice [June 2013] and the Human Rights Act 1998.

Any use of camera surveillance by the City of Wolverhampton Council that may be deemed to be covert and covered by this Policy will require authorisation.

Use of Wolverhampton UTC is controlled via the UTC Procedural Manual and Code of Practice. Any use by the City of Wolverhampton Council that may be deemed to be covert surveillance covered by this Policy will require authorisation.

Any requests received from external agencies to redirect cameras owned by the City of Wolverhampton Council, shall be forwarded to the Senior Responsible Officer for consideration.

3.7 Management of Investigations involving Social Media

If an investigation involves the potential use of information available on Social Media sites, officers shall have regard to the Councils Social Media in Investigations Policy **Appendix 6**

3.8 Wolverhampton Homes – Anti-social Behaviour Team

The Council retains overall responsibility for any surveillance activities undertaken by third parties assuming the Council's functions, such as Wolverhampton Homes which is an Arm's Length Management Organisation [ALMO] managing the Councils housing stock, such activity will be covered by this Policy.

Any application for directed surveillance or use of a CHIS by organisations assuming the Council's functions must be approved by an Authorising Officer of the Council in the normal manner and all activity will be recorded in the Council's Central Record.