

Cabinet – 15 July 2020

Surveillance and Access to Communications Data

Portfolio: Councillor Perry, Communities, Leisure and Culture

Related portfolios: The Leader of the Council

Service: Resilient Communities

Wards: All

Key decision: No

Forward plan: No

1. Aim

- 1.1. This report is presented to Cabinet to report members on the use of the powers contained in the Regulation of Investigatory Powers Act 2000 (RIPA 2000) and the Investigatory Powers Act 2016 (IPA 2016) with regard to surveillance and acquisition of communications data. It reports on the outcome of the inspection carried out by the Investigatory Powers Commissioner's Office on 28 January 2020 and further informs members of the draft new policies on these matters that will be presented for adoption at the next full meeting of Council.

2. Summary

- 2.1. On 28 January 2020, the Investigatory Powers Commissioner's Office carried out an inspection of Walsall Council and its use of RIPA. They confirmed that the recommendations of the previous inspection had been discharged. They made two recommendations and two observations on this inspection, These are detailed in paragraphs 4.6 to 4.9 below and they highlighted a number of areas of good practice which are detailed in paragraph 4.10. The RIPA policy has been updated to reflect changes in legislation and supplemented by a separate IPA policy. These need to be referred to full Council for adoption.

3. Recommendations

- 3.1 That Cabinet notes the use of the Regulation of Investigatory Powers Act 2000 for the years ending 31 March 2017, 31 March 2018, 31 March 2019 and 31 March 2020 and is assured by the Executive Director Economy Environment and Communities, as the Council's Senior Responsible Officer for this legislation, that usage is consistent with the Council's Policy and Procedures.
- 3.2 That the draft Corporate Policy and Procedures on the Regulation of Investigatory Powers Act 2000 be presented to Council for approval.

- 3.3 That the draft Corporate Policy and Procedures on the Investigatory Powers Act 2016 on the Acquisition of Communications Data be presented to Council for approval.
- 3.4 That the Executive Director Economy Environment and Communities is delegated authority to make administrative amendments to the policies as part of the report to Council.

4. Report detail - know

Context

- 4.1. Where there is an interference by a local authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the RIPA 2000 Act and IPA 2016 may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.
- 4.2 The Home Office has strongly recommended that local authorities seek an authorisation where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation ensures that the action is carried out in accordance with law and subject to stringent safeguards against abuse.
- 4.3 Directed surveillance authorisations under RIPA 2000 may be granted in relation to covert surveillance undertaken in relation to a specific investigation or operation which is likely to result in the obtaining of private information about a person, and which is other than an immediate response to events or circumstances and for the use of Covert Human Intelligence Sources (CHIS). Authorisations under IPA 2016 may be granted for the acquisition of certain communications data.
- 4.4 Table 1 below summarises the authorisations which have been granted in Walsall for the last 5 financial years. Due to the introduction of the serious crime threshold, the use has in reality been limited to trading standards investigations into the sale of age restricted goods and counterfeiting. Other surveillance activities which were previously conducted by the use of RIPA have either ceased or are conducted overtly. In certain circumstances, surveillance may be carried out that is not within the scope of the RIPA regime. However, in these circumstances, the same considerations are applied to ensure the activity is necessary and proportionate. An example of such activity is the use of covert recording for the operations to ensure hackney carriage and private hire drivers are complying with appropriate legislation when conveying passengers with disabilities.

| | | | | |
|--|-----------------|-----------------|-----------------|-----------------|
| Regulatory Services – age restricted sales test purchasing (eg cigarettes, alcohol), counterfeit goods | Y/E 31/03/17 | Y/E 31/03/18 | Y/E 31/03/19 | Y/E 31/03/20 |
|--|-----------------|-----------------|-----------------|-----------------|

| | | | | |
|---|---|---|---|---|
| Directed Surveillance Authorisations | 2 | 3 | 6 | 1 |
| Covert Human Intelligence Source Authorisations | 0 | 0 | 0 | 0 |

Table 1 RIPA authorisations 2016/17 to 2019/20

- 4.5 On the 28 January 2020, the Investigatory Powers Commissioner's Office (IPCO) carried out an inspection of Walsall Council. The inspection report and Commissioner's covering letter are attached as **Appendix 1**. The report confirms that the recommendations from the previous inspection carried out in June 2016 have been discharged. The report makes two new recommendations and two observations.
- 4.6 Recommendation R1 is that elected members are informed the use of RIPA and set the policy yearly. This report fulfils that recommendation.
- 4.7 Recommendation R2 is to ensure sufficient detail is included in the application and authorisation. Once the revised policy is adopted and the new service structure for Resilient Communities put in place, refresher training will be provided for front line officers who undertake investigations and for the Authorising Officer. In the meantime, feedback has been given to the officers who complete applications.
- 4.8 Observation O1 is a note of good practice that authorisations are cancelled in a timely manner when the authorisation is no longer required.
- 4.9 Observations O2 concerns surveillance which is conducted otherwise than under the auspices of RIPA. Although full consideration and management strategies were in place to cover all aspects of the risks identified, they were not all recorded.
- 4.10 The inspector commended Walsall Council on its use of RIPA and highlighted a number of areas of good practice, including:
- Inviting managers of services who currently do not need to use RIPA for their work to attend training to ensure they are aware of the provisions and do not inadvertently breach the requirements.
 - The use of the principles of RIPA when carrying out surveillance for investigations which would fall within scope other than they do not meet the serious crime threshold.
 - Cancellations of authorisations in a timely manner when they were no longer needed.
 - Comprehensive codes of practice on the use of directional CCTV.
 - Awareness of the potential benefits of the use of RIPA in the digital age.

- 4.11 The Walsall Council Policy and Procedures on the Regulation of Investigatory Powers Act 2000 has been rewritten to reflect changes in the legislation and the codes of practice, as well as some organisational changes. The draft proposed policy is attached as **Appendix 2**.
- 4.12 Those elements of the previous policy which relate to the acquisition of communications data have been separated out into a new policy to reflect changes in the legislation, the codes of practice, organisational changes and for ease of understanding. The draft proposed Policy and Procedures on the Investigatory Powers Act 2016 on the Acquisition of Communications Data is attached as **Appendix 3**.

Council Corporate Plan priorities

- 4.13 By using the tools and powers in the legislation which is enforced by officers within the Regulatory Services teams of Walsall Council legally, the teams support the corporate priorities to ensure that:
- children are safe from harm and healthy for example in restricting the illegal sale of age restricted goods such as alcohol and tobacco;
 - there is economic growth for all people, communities and businesses for example by investigating and restricting the supply of illicit and unsafe goods;
 - communities are prospering and resilient in safe and healthy places that build a strong sense of belonging and cohesion for example by ensuring communities are protected from crime linked to organised crime groups or from the disruption caused by children who have been drinking under age.

Risk management

- 4.14 Where there is an interference by a local authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 and 2016 Acts may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998. Failure to follow the procedures set out in the legislation and the Council's Policies (**Appendices 1 and 2**) may result in the Council's actions being deemed unlawful and consequently lead to claims for compensation, loss of reputation and information being ruled inadmissible in a prosecution action. Adherence to these Acts also provides an additional layer of protection under the Data Protection Act 2018 and the General Data Protection Regulations 2016. These risks are mitigated by the adoption of the policies and training of staff.

Financial implications

- 4.15 The financial implications of these procedures are in training of staff which is met from existing revenue budgets. There is a financial risk of failing to adhere to the 2000 and 2016 Acts in that it may lead to claims for compensation.

Legal implications

- 4.16 The legislation which is enforced by the teams within Regulatory Services contains tools and powers to enable them to investigate criminal offences. The 2000 and 2016 Acts provide some controls on the use of these powers. The legal implications of failing to follow these requirements is the same as is outlined in the risk management section described at paragraph 4.5 above.

Procurement Implications/Social Value

- 4.17 There are no procurement implications to this report.

Property implications

- 4.18 There are no property implications to this report.

Health and wellbeing implications

- 4.19 By using the 2000 and 2016 Acts appropriately, services are able to investigate criminal offences. This ensures that the Marmot objectives are met by protecting people at all life stages and promoting a fair and safe environment in which business can thrive.

Staffing implications

- 4.20 The only staffing implications relevant to this report is in the provision of training to officers.

Reducing Inequalities

- 4.21 The implications for reducing inequalities have been taken into account. The approvals process requires that all the circumstances of any persons identified are taken into account in each case. An equalities impact assessment (EqIA) has been carried out and is attached to this report as Appendix 3

Consultation

- 4.22 Consultation has been undertaken with legal services, finance, public health, human resources and communications. External consultation is not required for this report.

5. Decide

- 5.1 This report is to enable members of cabinet to present the draft proposed policies to Council in order that they can be formally adopted to mitigate the risks identified in paragraph 4.13.

6. Respond

- 6.1 If cabinet accept the recommendations, a report will be presented to full Council on 19 May 2020 to adopt the draft policies.

7. Review

- 7.1 The Senior Responsible Officer provides oversight on the use of RIPA and IPA. A annual report will be presented to members as required in the Surveillance Code of Practice.

Background papers

There are no additional papers for this report.

Author

Lorraine Boothman
Regulatory Services Manager
☎ 653065

✉ Lorraine.boothman@walsall.gov.uk

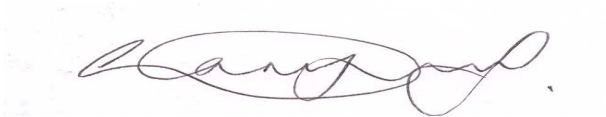


Simon Neilson
Executive Director Economy
Environment and Communities

7 July 2020

David Elrington
Regulatory Services Manager
☎ 653023

✉ david.elrington@walsall.gov.uk



Councillor Perry
Communities Leisure and Culture

7 July 2020



Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Dr H Paterson
Chief Executive
Walsall Metropolitan Borough Council

12 February 2020

Dear Dr Paterson,

IPCO Inspection report – Walsall Metropolitan Borough Council

On the 28 January 2020 one of my Surveillance Inspectors, Mrs Samantha Jones, examined the arrangements made by Walsall Metropolitan Borough Council to secure compliance with the legislative provisions which govern the use of covert surveillance, the management of covert human intelligence sources and the acquisition of communications data. I have attached the report that was compiled following the inspection, which I endorse.

The previous two recommendations highlighted from the inspection undertaken by Sir David Clarke, Assistant Commissioner, in June 2016 have been addressed and discharged, albeit a further recommendation has been made regarding the policy documents being ratified by Elected Members on an annual basis. There is a second recommendation relating to the authorising officer's considerations, which should be fully compliant with legislative requirements. There is also one additional observation in relation to authorisations sought outside of the protection of the Act. I would be grateful if you could ensure these matters are addressed at the earliest opportunity. I am also pleased to highlight the area of good practice identified, for the promptness in which cancellations are sought when authorisations are no longer necessary or proportionate.

I take the opportunity here to remind you of the importance of regular, ongoing internal oversight of the actual or potential use of these powers, which should be managed through the Senior Responsible Officer. Officers need to maintain their levels of training, particularly when the powers are used sparingly. I hope that you find the inspection report to be helpful and constructive. My Office is available to you should you have any queries following the recent inspection, or at any point in the future. Contact details are provided at the foot of this letter.

I shall be grateful if you would acknowledge receipt of the report, and your plans in relation to its findings, within one month.

Yours sincerely

A handwritten signature in black ink that reads 'Brian Leveson'.

The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner



Inspection Report – Walsall Metropolitan Borough Council

Contents

| | | |
|-----|---|---|
| 1 | Introduction | 2 |
| 2 | Inspection methodology | 2 |
| 3 | Key findings..... | 3 |
| 3.1 | Recommendations | 3 |
| 3.2 | Observations | 3 |
| 4 | Actions taken on previous inspection recommendations..... | 4 |
| 5 | Inspection findings..... | 4 |
| 5.1 | Policy and Procedures..... | 4 |
| 5.2 | Surveillance | 5 |
| 5.3 | Covert Human Intelligence Sources (CHIS) | 6 |
| 5.4 | Communications Data (CD)..... | 7 |
| 6 | Conclusion | 7 |
| 7 | List of records reviewed | 8 |

1 Introduction

- 1.1 This inspection has been conducted to assess the level of compliance of Walsall Metropolitan Borough Council with the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 in respect of its use and management of covert surveillance, covert human intelligence sources and communications data. The most recent inspection of Walsall MBC was undertaken by Sir David Clarke, Assistant Surveillance Commissioner in June 2016.
- 1.2 This inspection took place on 28 January 2020 and was conducted by IPCO Inspector, Mrs Samantha Jones.
- 1.3 This report is addressed to the Chief Executive, Dr Helen Paterson, whose address for correspondence is Civic Centre, Darwell Street, Walsall, West Midlands, WS1 1TP. The report can be emailed to the following email address: Helen.Paterson@walsall.gov.uk
- 1.4 The Senior Responsible Officer is Executive Director, Mr Simon Neilson, email address: Simon.Neilson@walsall.gov.uk

2 Inspection methodology

- 2.1 In the period since the last inspection Walsall MBC has used the powers afforded to it under the legislation to conduct directed surveillance only. Therefore, the inspection comprised a dip sample of the surveillance authorisations, and a review of the policy documents, training records and discussions with key staff involved in the process.
- 2.2 Statistics relating to what was viewed at this inspection are captured in
- 2.3 Table 1 below. Please see Section 7 for a full list of which records were viewed during the inspection.

| For the period: April 2016 – December 2019 | | | |
|--|--|---|------------------------------------|
| Walsall Metropolitan Borough Council | Total authorisations in current reporting period | Total authorisations in previous reporting period | Total records viewed at Inspection |
| Directed Surveillance | 12 ¹ | 15 | 7 |
| CHIS | 0 | 0 | 0 |

Table 1. Key Statistics

¹ Thirteen applications were submitted and authorised, one was withdrawn prior to submission to the Court.

2.4 The persons interviewed during the course of the inspection are captured in Table 2 below.

| Persons Interviewed |
|---|
| Paul Green – Legal Services |
| Lorraine Boothman – Regulatory Services Manager |
| David Elrington – Regulatory Services Manager |
| Ken Pattern – Locality and Partnerships |
| Helen Kindon – Manager, Locality and Partnerships |
| Stuart Powell – Team Leader, Trading Standards |
| Steve Doyle – Senior Trading Standards Officer |

Table 2. Persons interviewed

3 Key findings

3.1 Recommendations

3.1.1 There are two formal recommendations arising from the inspection.

| Number | Reference | In relation to | Recommendation | Recommendation type |
|---------------|------------------|------------------------|---|---|
| R1 | 5.1.3 | Elected Members | Elected Members should be formally sighted on the authority's use of the legislation and set policy at least once a year (Surveillance Code of Practice para. 4.47) | Recommendation – observed potential for improvement |
| R2 | 5.2.2 | Surveillance | To ensure authorisations contain all the necessary statutory requirements | Recommendation – observed potential for improvement |

Table 3. Key recommendations resulting from inspection

3.2 Observations

3.2.1 The key observations arising from the inspection are listed in Table 4 below.

| Number | Reference | In relation to | Observation | Observation type |
|---------------|------------------|-----------------------|---|-------------------------|
| O1 | 5.2.3 | Surveillance | Authorisation are cancelled promptly when no longer required. | Good practice |
| O2 | 5.2.5 | Non RIPA | All relevant legislation to be considered prior to undertaking covert activity. | Observation |

Table 4. Key observations resulting from inspection

4 Actions taken on previous inspection recommendations

- 4.1 **R1:** *That WC's RIPA Policy be further revised in accordance with paragraph 10 of this report.*

Discharged: The RIPA policy was amended following the previous inspection to include a section on social networks and was last put before Elected Members in September 2017. The current policy, albeit in draft format, has been split to form two separate policies; a policy for activity conducted under RIPA (surveillance and CHIS), and activity under the Investigatory Powers Act (IPA) (communications data acquisition). These are comprehensive documents that fulfil the necessary requirements but will need to be ratified by Elected Members.

R2: *That in both RIPA training and investigation practice, specific attention is paid to the circumstances in which RIPA authorisation of directed surveillance and/or CHIS is required so as to avoid any risk of unauthorised infringement of privacy.*

Discharged: The policy documentation, training undertaken in 2017, and discussions with staff during the inspection process highlighted the knowledge of what circumstances and when authorisation, be it CHIS and/or directed surveillance, is necessary.

5 Inspection findings

5.1 Policy and Procedures

- 5.1.1 The Chief Executive is Dr Helen Paterson, having replaced Mr Paul Sheenan in November 2017. Dr Paterson remains as the authorising officer in respect of the enhanced level authorisations specified in annex A of the Codes of Practice. There are four Executive Directors in support, one of whom, the Executive Director Economy and Environment, Mr Simon Neilson, is the Senior Responsible Officer and currently acts in a temporary capacity as the authorising officer. Whilst this is not an ideal situation, it is a temporary solution following the departure of Dr Barbara Watts, a long serving AO, and an imminent restructuring of senior management across all services. Once this restructure has been finalised and put before the Personnel Committee, a Head of Service will be identified as the next substantive authorising officer.
- 5.1.2 Unfortunately, it was not possible to meet with either the Chief Executive or the SRO on the day of the inspection due to their absence for personal reasons.

5.1.3 Since the update to policy following the 2016 recommendation, the policy document(s) had not been revised until recently and currently sit in a draft format. No further formal representations have been made to the Elected Members since 2017. In order to comply with paragraph 4.47 of the Surveillance Code of Practice, Elected Members of the authority are required to review the use of the legislation by the council and agree policy at least once a year.

5.1.4 A comprehensive record of external training undertaken by relevant Walsall MBC personnel is maintained and highlights that training is undertaken on a semi regular basis (the last being in 2017). The process is based on what external training is available. A further training session is planned for 2020 following the restructure, to ensure all relevant staff are identified and trained accordingly. It is also pleasing to note that managers of other departments, although unlikely to use the powers, are encouraged to attend training sessions in order to ensure there is awareness of what potentially constitutes activity that should be afforded the protection of RIPA.

5.2 Surveillance

5.2.1 All authorisations granted for directed surveillance were either for underage sales of tobacco and/or alcohol or the sale of illicit tobacco. All bar one (in November 2019) were authorised by the same authorising officer, who is no longer employed by Walsall MBC. In general, applications were well explained and addressed the key principles, but when looked at in succession became very much ‘templated’ without giving due consideration to the uniqueness of each individual premises visited.

5.2.2 The input from the authorising officer was handwritten and in the main compliant with the requirements of RIPA and the Code of Practice. However, the following was highlighted:

- Neither the premises nor any subjects were specifically referred to, just as a reference to the section in the application
- The duration of an authorisation is set down in the legislation and cannot be altered, however on most of the authorisations the expiry date was incorrect
- It was noted on two of the authorisations that the delay in presenting the authorisation to a local magistrate was approximately three weeks. This process should be reviewed to ensure timeframes are conducive in ensuring compliance with the requirements of the Codes of Practice
- Within URN RIPA 21, the reasoning as to why it was withdrawn prior to approval from a magistrate was not evident, with no consideration being given to cancelling the authorisation
- Cancellations did not contain any detail as to any retention and deletion of product, despite this being highlighted as an observation at the previous inspection in 2016.

5.2.3 The cancellations in all the authorisations viewed were submitted in a timeous fashion as soon as deployments had ceased; this is to be applauded.

- 5.2.4 Walsall MBC has comprehensive codes of practice and procedural documentation in place to ensure that the directional use of CCTV and/or any request from law enforcement or local authorities/partner agencies to view any CCTV as part of a directed surveillance authorisation is fully compliant with the legislation. It was highlighted that one request had been made in the period since the last inspection, which was refused because an authorisation was not in place.

Non- RIPA

- 5.2.5 Walsall MBC undertakes surveillance activity which would fall under the RIPA legislation if not for the fact that the offences under investigation would not meet the criterion of a maximum sentence of six months or more. One such authorisation was examined and concerned the audio and visual recording of a taxi journey to ensure that the legal requirements when transporting a person in a wheelchair were met. No consideration had been given in the application or subsequent approval by the authorising officer as to whether this interaction would require an authorisation under the legislation governing the use of CHIS, to which the crime threshold does not apply. When discussing this in the feedback, it was evident that this had been considered, with a passive role being undertaken and parameters around conversation management agreed, however this was not detailed in any of the associated paperwork.

5.3 Covert Human Intelligence Sources (CHIS)

- 5.3.1 There have been no authorisations for the use and conduct of a CHIS. This reflects the widespread practice common amongst local authorities of never or rarely authorising CHIS. However, the possibility of utilising a CHIS in the near future, for a specific operation, with collaboration from neighbouring councils and the National Markets Group was discussed. Should this go ahead, assurances were provided that the necessary statutory requirements would be fulfilled.
- 5.3.2 The possibility of status drift was discussed in relation to monitoring information provided by members of the public. Managers are alive to the possibility and are confident that sufficient awareness exists amongst staff and processes in place to be alerted to any potential status drift.
- 5.3.3 At present any online activity is conducted overtly using clearly attributed council profiles. One covert profile on a non-attributed computer is utilised to conduct monetary transactions on open source websites such as eBay or on Instagram, with no further interaction taking place. The staff spoken to are fully alive to the potential of CHIS relationships and the drift into directed surveillance territory should routine monitoring take place.

5.4 Communications Data (CD)

- 5.4.1 Walsall MBC has not made any application to acquire communications data (CD) during the reporting period but is registered with the National Anti-Fraud Network (NAFN) and has processes in place to do so if required. The acquisition of CD now falls under Chapter 3 of the Investigatory Powers Act 2016 (IPA) which places local authorities on the same standing as the police and law enforcement agencies. Previously, local authorities had been limited to obtaining subscriber details (now known as “entity” data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as “events” data and has long played a vital role in criminal investigations.
- 5.4.2 A new threshold for which CD “events” data can be sought has been introduced under the IPA as “applicable crime”. Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person’s privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of the CD Code of Practice.
- 5.4.3 The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA).
- 5.4.4 Walsall MBC is fully cognisant of these changes and is updating its RIPA Policy document accordingly.

6 Conclusion

- 6.1 While the powers afforded to Walsall MBC have been used sparingly since the last inspection, the potential benefits to an investigation, particularly in the digital age, has been highlighted. There are two formal recommendations, and to ensure continuing compliance there is also one observation which, if not remedied, could manifest, should intervention not be conducted at this stage. One area of good practice has also been highlighted.
- 6.2 Particular thanks should be given to Yvonne Boon, who made all the arrangements for the inspection and provided comprehensive reading material in advance.

7 List of records reviewed

7.1 For completeness, a full list of all records viewed during the inspection is captured below in table 5.

7.2 Records listed here may have been viewed fully or only in part depending on the inspection methodology and approach taken.

| Total records viewed at Inspection per power | Operation URN |
|--|---------------|
| Directed Surveillance (7) | RIPA 23 |
| | RIPA 22 |
| | RIPA 21 |
| | RIPA 20 |
| | RIPA 19 |
| | RIPA 18 |
| | RIPA 17 |

Table 5. List of records viewed

Samantha Jones
IPCO Inspector



Walsall Council

Regulation of Investigatory Powers Act 2000

Surveillance and Covert Human Intelligence Source Policy and Procedure

Page left intentionally blank

Contents

| | | |
|---|---|----|
| | Glossary | 4 |
| 1 | Policy Statement | 5 |
| 2 | Legislative background | 7 |
| 3 | Surveillance | 8 |
| 3.2 | Overt Surveillance | 8 |
| 3.3 | Covert Surveillance | 8 |
| 3.6 | Covert Directed Surveillance | 9 |
| 3.7 | Directed Surveillance Crime Threshold | 9 |
| 3.9 | Covert Intrusive Surveillance | 9 |
| 3.13 | Non RIPA Authorisations | 10 |
| 4 | Private Information | 11 |
| 5 | Confidential Information | 12 |
| 6 | Covert Human Intelligence Source CHIS | 13 |
| 7 | Vulnerable Individuals/Juvenile CHIS | 13 |
| 8 | CCTV | 14 |
| 9 | Use of Social Media/Internet | 14 |
| 10 | Aerial Surveillance | 16 |
| 11 | Residential Premises & Private Vehicles | 16 |
| 12 | Restrictions on Certain Activities | 17 |
| 13 | Authorisation Procedures | 17 |
| 13.1 | Authorising Officers for Directed Surveillance and CHIS | 17 |
| 13.7 | Authorisation of Covert Directed Surveillance and Use of a CHIS | 18 |
| 14 | The Magistrates Court | 19 |
| 15 | The procedure for applying for directed surveillance or use of a CHIS | 20 |
| 16 | Additional Requirements for Authorisation of a CHIS | 21 |
| 17 | Urgent Authorisations | 21 |
| 18 | Review of Authorisations | 21 |
| 19 | Renewal of Authorisations | 22 |
| 20 | Cancellation of Authorisations | 22 |
| 21 | What Happens if Surveillance has Unexpected Results | 22 |
| 22 | Errors | 23 |
| 23 | Records of RIPA Authorisation | 23 |
| 24 | Handling of Material and Safeguards | 24 |
| 25 | Use of Material as Evidence | 25 |
| 26 | Disseminating Material | 26 |
| 27 | Copying Material | 26 |
| 28 | Storage of Material | 26 |
| 29 | Retention and Destruction of Material | 26 |
| 30 | Surveillance Products | 27 |
| 31 | Training and advice and departmental policies, procedures and codes of conduct. | 27 |
| 32 | Complaints | 28 |
| APPENDIX 1 Non RIPA Authorisations - Forms | | 29 |
| APPENDIX 2 List of Authorised Officer Posts for Authorising Directed surveillance | | 44 |
| APPENDIX 3 LEGISLATION | | 45 |

Glossary

| | |
|------|---|
| ANPR | Automated Number Plate Recognition |
| AO | Authorising Officer |
| CCTV | Closed Circuit Television. |
| CHIS | Covert Human Intelligence Source. |
| DVLA | Driver and Vehicle Licensing Agency |
| ECHR | European Contention on Human Rights |
| HRA | Human Rights Act 1998. |
| JP | Justice of the Peace |
| IPCO | Investigatory Powers Commissioners Office |
| RIPA | Regulation of Investigatory Powers Act 2000 |
| SNS | Social Network Sites |
| SRO | Senior Responsible Officer. |

1. Policy Statement

- 1.1 The objective of this policy and procedure is to ensure that all investigations within the scope of the Regulation of Investigatory Powers Act 2000 ('RIPA'), as amended and the Codes of Practice issued by the Home Office are carried out effectively and are properly authorised. In addition it provides guidance to officers and elected members on the requirements and outlines the procedures to be followed in utilising their investigatory powers.

This document should be in conjunction with the legislation and the Home Office's Codes of Practice.

- 1.2 The activities covered by this policy and guidance document are:

- covert surveillance
- the use of covert human intelligence sources (CHIS)

These investigatory powers should only be used in circumstances where it is necessary and proportionate having considered all the requirements of the legislation, codes of practice and this policy. The legislation and codes should be consulted from time to time, and at annual review to ensure this document remains up-to-date.

1.4 What RIPA Does and Does Not Do

RIPA does:

- Require prior authorisation of directed surveillance.
- Prohibit the council from carrying out intrusive surveillance.
- Require authorisation of the conduct and use of CHIS.
- Require safeguards for the conduct of the use of a CHIS.

RIPA does not:

- Make unlawful conduct which is otherwise lawful.
- Prejudice any existing power to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a property.
- Apply to activities outside the scope of Part II of RIPA, which may nevertheless be governed by other legislation, including the HRA. A public authority will only engage RIPA when in performance of its 'core functions' – i.e. the functions specific to that authority as distinct from all public authorities.

- 1.5 Further guidance on the requirements of the legislation, the codes of practice and this policy can be obtained from the Legal Services team of Walsall Council.
- 1.6 The requirements of RIPA as supported by this document, are important for the effective and efficient operation of the council's actions with regard to Covert Surveillance and Covert Human Intelligence Sources. This policy and procedure document will therefore be kept under annual review by the Executive Director of Economy & Environment, who is the nominated Senior Responsible Officer (SRO) for the purpose of RIPA. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Executive Director for Economy & Environment at the earliest opportunity.
- 1.7 In circumstances where RIPA does not apply, this does not mean that surveillance cannot be undertaken, but it must be carried out with due regard to all legal requirements, giving due attention to the necessity, reasonableness and proportionality tests (and relevant articles of ECHR) see 3.13.
- 1.8 This policy and guidance document will be considered by Cabinet on an annual basis and this report will include a review of the use of RIPA by the organisation. Where changes are required to the Policy either because of updates to legislation, codes of practice or other guidance the Policy and details of the use to which it has been put will be considered by Cabinet before progressing for approval and adoption by full Council. Delegation has been given to the Senior Responsible Officer for minor amendments to the policy, eg to reflect changes in officers or structural changes to the organisation or other amendments which do not impact on the policy itself.
- 1.9 **Consequences of Failing to Comply with this Policy**

Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA and this Policy may result in the Council's actions being deemed unlawful. This could in turn lead to claims for compensation, loss of reputation and in certain circumstances any information obtained that could be of help in a prosecution will be inadmissible.

2. Legislative Background

- 2.1 On 2 October 2000 the Human Rights Act 1998 (“HRA”) made it unlawful for a local authority to breach any article of the ECHR. An allegation that the Council or someone acting on behalf of the Council has infringed the ECHR is dealt with by the domestic courts rather than the European Court of Justice.

The ECHR states:

- a) individuals have the right to respect for their private and family life, home and correspondence (Article 8 ECHR); and
 - b) there shall be no interference by a public authority with the exercise of this right unless that interference is:
 - in accordance with the law;
 - necessary; and
 - proportionate
- 2.2 RIPA, which came into force on 25 September 2000, provided a lawful basis for three types of investigatory activity to be carried out by local authorities which might otherwise breach the ECHR. The activities were:
- a) covert surveillance;
 - b) covert human intelligence sources (“CHIS”); and
 - c) acquisition and disclosure of communications data.

This regime was further refined with the introduction of the Investigatory Powers Act 2016 (IPA). From April 2019, while the first two investigatory techniques above remained within RIPA and are still current, the legislative powers and controls relating to the acquisition and disclosure of communications data moved to the IPA. There is a separate policy within Walsall Council governing the acquisition of communications data under IPA.

- 2.3 RIPA set out procedures that must be followed to ensure the activity is lawful. Where properly authorised under RIPA, the activity will be a justifiable interference with an individual’s rights under the ECHR; if the interference is not properly authorised an action for breach of the HRA could be taken against the Council, a complaint of maladministration made to the Local Government Ombudsman or a complaint made to the Investigatory Powers Tribunal.
- 2.4 In addition, if the procedures are not followed any evidence collected may be disallowed by the courts. RIPA seeks to balance the rights of individuals against the public interest in the Council being able to carry out its statutory duties.

3. Surveillance

3.1 Surveillance can be defined as “overt”, “covert”, “directed” and “intrusive” and includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- Recording anything mentioned above in the course of authorised surveillance.
- surveillance, by or with, the assistance of appropriate surveillance device (s).

3.2 Overt Surveillance

The majority of the Council’s surveillance activity will be overt surveillance i.e. will be carried out openly. For example

- where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted;
- where the Council advises a resident that their activities will be monitored as a result of neighbour nuisance allegations
- or where an officer uses body worn cameras and informs the individual that the camera will be switched on and recording will take place. This type of overt surveillance is normal Council business and is not regulated by RIPA.

3.3 Covert Surveillance

This is where surveillance is carried out in a way that ensures that the person subject to the surveillance is unaware it is taking place.

3.4 Where covert surveillance activities are unlikely to result in obtaining of any private information about a person (because the surveillance although covert is general or low level, and is not directed at particular individuals), no interference with Article 8 rights occurs, and an authorisation under RIPA is not required.

3.5 RIPA authorisation may however be required where the surveillance is repeated for a particular purpose and could amount to systematic surveillance of an individual; if in doubt advice should be sought from Legal Services.

3.6 **Covert Directed Surveillance**

Surveillance that is:

- covert
- not intrusive;
- for the purposes of a specific investigation or operation;
- likely to obtain private information about a person (whether or not that person was the target of the investigation or operation); and
- not carried out as an immediate response to events or circumstances which could not have been foreseen prior to the surveillance taking place

3.7 **Directed Surveillance Crime Threshold**

Following the changes to RIPA introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 a crime threshold applies to the authorisation of directed surveillance by local authorities.

3.8 Authorising Officers (AO's) may not authorise directed surveillance unless it is for the purpose of preventing or detecting a criminal offence AND meets the following:

- The criminal offence is punishable by a maximum term of at least 6 months imprisonment, or
- involves the sale of tobacco and alcohol to underage children which is an offence under sections 146, 147, or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1993 (offences).

3.9 **Covert Intrusive Surveillance**

Local authorities cannot lawfully carry out covert intrusive surveillance however to assist in decision making the following section describes what covert intrusive surveillance is.

3.10 Covert intrusive surveillance takes place when covert surveillance is carried out in relation to anything taking place on residential premises or in a private vehicle.

3.11 It also involves the presence of an individual or surveillance device on the premises or in the vehicle, or the use of a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as expected of a device placed inside.

3.12 Additionally, the Regulation of Investigatory Powers (Extension of Authorisations Provisions: Legal Consultations) Order 2010 states that covert surveillance carried out in relation to anything taking place in certain specified premises is intrusive when they are being used for legal consultation. These places include:

- any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained
- any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007
- police stations
- any place in which persons may be detained under Part VI of the Criminal Procedures (Scotland) Act 1985, the Mental Health (Care and Treatment) (Scotland) Act 2003 or the Mental Health Act 2003
- the place of business of any professional legal adviser; and
- any place used for the sittings and business of any court, tribunal, inquest or inquiry

3.13 Non RIPA Authorisations

3.14 Some activity is not classed as directed surveillance and no authorisation is required nor can be given for that activity for example.

- Covert surveillance in immediate response to events. Where officers are carrying out their routine duties and an incident occurs that they decide to follow and it is not reasonably practicable to be expected to obtain an authorisation, then an authorisation is not required.
- Covert surveillance as part of general observation work. Where officers are carrying out routine work, such as walking through town to ensure there are no breaches of legislation which they enforce, monitoring publicly accessible parts of the internet which are not part of a specific investigation, then this is not classed as covert surveillance.
- Covert surveillance not related to the statutory grounds or core activities of the Authority. RIPA authorisation is only required for specific investigations or operations where it is necessary on the grounds specified in s28(3) of the 2000 Act. Covert surveillance carried out for any other purpose should be conducted in accordance with the relevant legislation and RIPA authorisation is not required. RIPA is required for core functions that are specific to that authority, e.g. the work of enforcement teams within the Council. General activities that are carried out by all authorities, eg employment issues, are classed as ordinary functions and not subject to RIPA.

However, other legislation such as the Human Rights Act, General Data Protection Regulations may apply.

- Overt use of CCTV and ANPR systems. CCTV systems are used by the Council in a number of situations and the public are normally made aware that they are in use. RIPA authorisation is not normally required where these systems are used for the general monitoring of the area or to review an incident and gather evidence of a crime after it has happened.

However where the system is used in a covert manner to monitor a particular subject as part of a planned operation, this becomes directed surveillance and a RIPA authorisation should be obtained.

- Covert surveillance as part of an equipment interference warrant. Where a warrant has been obtained under part 5 of the 2016 Act, then a separate RIPA authorisation is not required.
- Recording equipment worn by a CHIS. Where a CHIS acting under a conduct authorisation wears a recording to record information obtained in their presence a separate RIPA authorisation is not required.
- Covert recording of noise recording sound levels only. A RIPA authorisation is not required where a covert noise recording device records only sound levels; machinery, music or other non-verbal noise; or verbal content is recorded at a level which does not exceed that which can be heard in the street outside or adjoining the property with the naked ear.

- 3.15 Where investigating Officers are undertaking surveillance, examples of which are given above (3.14), they should still give consideration to the necessity and proportionality of the surveillance and seek authorisation from an AO to proceed.
- 3.16 The appropriate 'Application for authorisation to carry out directed surveillance' forms at **APPENDIX 1** should be completed, authorised and stored securely by the relevant AO.

4 Private Information

- 4.1 The 2000 Act states that private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.
- 4.2 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

- 4.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites (see 7).
- 4.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

Practical examples of these differing scenarios can be found in the [Code of Practice for Covert Surveillance and Property Interference](#) on the Home Office website.

5. Confidential Information

- 5.1 A higher level of authorisation to apply to the Magistrates Court is required in relation to RIPA activity when the subject of the investigation might reasonably expect a high degree of privacy, or where "confidential information" might be obtained. For the purpose of RIPA this includes:
- communications subject to legal privilege
 - communications between a member of parliament and another person on constituency matters;
 - confidential personal information and
 - confidential journalistic material
- 5.2 The AO and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure. Authorisation can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service.
- 5.3 Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from Legal Services prior to making any application.

6. Covert Human Intelligence Sources (“CHIS”)

- 6.1 The Council is permitted to use CHIS subject to strict compliance with RIPA.
- 6.2 A CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:
- (a) covertly using the relationship to obtain information or provide access to information to another person, or
 - (b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.
- 6.3 A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council’s behalf. Authorisation for CHIS can only be granted if it is for the purposes of preventing or detecting crime or of preventing disorder.
- 6.4 Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.
- 6.5 However, by virtue of section 26(8) (c) of RIPA, there may be instances where an individual, who covertly discloses information though not tasked to do so may nevertheless be a CHIS.
- 6.6 The important question is how did the member of the public acquire the information which they volunteer? If they acquired it in the course of, or as a result of, the existence of, a personal or other relationship, they are likely to fall within the definition of a CHIS. If the Council then makes use of the information, and the informant is thereby put at risk, the Council may be in breach of its duty of care owed to the individual. It is recommended that legal advice is sought in any such circumstances.
- 6.7 The [Covert Human Intelligence Sources Code of Practice](#) can be found on the Home Office website.

7 Vulnerable Individuals / Juvenile CHIS

- 7.1 Although it is unlikely Walsall Council would use such persons additional requirements would apply to the use of a vulnerable individual or a person under the age of 18 as a CHIS. In both cases authorisation for an application to the Magistrates Court can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service.

Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from Legal Services prior to making the application.

- 7.2 The use or conduct of a CHIS under 16 years of age must not be authorised to give information against their parents or any person who has parental responsibility for them.
- 7.3 In other cases authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended in 2018) are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.
- 7.4 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves or protect themselves against significant harm or exploitation.

8. CCTV

- 8.1 The installation and use of unconcealed CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance requiring RIPA authorisation. However, there are specific provisions regulating the use of CCTV cameras in public places and buildings and the Council has drawn up a Corporate CCTV Policy which officers must comply with. However if CCTV cameras are being used in such a way that the definition of covert directed surveillance is satisfied, RIPA authorisation should be obtained.
- 8.2 For instance the use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation.

However, the use of the same CCTV system to conduct planned surveillance of an individual and record their movements is likely to require authorisation.

- 8.3 Protocols should be agreed with any external agencies requesting use of the Council's CCTV system. The protocols should ensure that the Council is satisfied that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

9. Use of Social Media / Internet

- 9.1 The internet may be utilised to obtain information including viewing specific user profiles on Social Networking Sites ('SNS'), or searching SNS to try to find profiles that contain useful information. Used correctly, research of SNS might provide invaluable evidence or at least useful intelligence.

- 9.2 Some activity on SNS might however constitute Directed Surveillance or require CHIS authorisation, some may not. Similarly some research might be likely to result in the obtaining of private information, some may not. Activity that does not meet the threshold for RIPA authorisation but might be likely to result in obtaining private information will require consideration of Human Rights issues such as balancing the protection of rights with the breach of privacy, necessity and proportionality.
- 9.3 It is important to note that images of persons are private information, and also for officers to be aware that it is possible they might obtain private information about other individuals not just the specific user on the profiles which are viewed, captured or recorded. These individuals might not even be aware this private information has been made public by the profile/account holder.
- 9.4 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy.
- 9.5 If it is necessary and proportionate for an officer to covertly record information from a SNS, the minimum requirement is an authorisation for directed surveillance.
- 9.6 An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a SNS and subsequently forms a relationship with them
- 9.7 Use of an established overt presence of the public authority on the SNS to look at publicly available information on the profile is possible and viable if the Council has a presence on the SNS which is used to publicly and overtly make the presence of the Council known, however this does not mean that information freely displayed on a profile is "fair game".
- 9.8 The first covert visit to an SNS profile which might be displaying lots of private information could be regarded as a 'drive by' however any subsequent covert visits, particularly on a regular basis are likely to require authorisation for directed surveillance if the Council is likely to obtain private information, and this would be obvious as a result of the initial visit.

10. Aerial Surveillance

- 10.1 Where surveillance is carried out using aircraft, whether manned, eg helicopters, or unmanned, eg drones, or other aerial devices then the same considerations need to be given to whether RIPA authorisation is needed as for any other type of surveillance. Particular consideration needs to be given to the reduced visibility and awareness of the device at height.

11 Residential Premises & Vehicles

- 11.1 Residential premises are defined as any premises for the time being occupied by any person, including on a temporary basis, for residential purposes or as living accommodation, including hotels. However, common areas to which a person has access in connection with that use are excluded. Residential premises occupied by a local authority for non-residential purposes are excluded. For example a house covertly used by trading standards to which traders are invited to carry out maintenance work or repair known faults, to discover if they are acting honestly. (A “house of horrors” set up.)

- 11.2 Examples of locations which are and are not classed as residential premises are given below:

Examples of locations classed as residential premises

- Rented flat
- Hotel bedroom or suite

Examples of locations not classed as residential premises

- Communal stairway in block of flats (unless used as temporary place of abode by a homeless person)
- Hotel reception or dining room
- Front garden of premises readily visible to the public
- House of horrors

- 11.3 **Private vehicles** are defined as a vehicle, including a vessel, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or having the right to use it. This includes a company car used for business and pleasure of an employee.

- 11.4 The use of a tracking or recording device in vehicles owned by a local authority is unlikely to be covert if members of staff are informed of that use. However, if they are used for a purpose that the employee has not been informed of, or for the purpose of covertly monitor, record, observe, listen to the occupants, then that may require authorisation.

12. Restrictions on Certain Activities

12.1 Local Authorities are not permitted within the legislation to undertake certain activities including:

- interference with private property e.g. placing tracking devices on private vehicles
- carrying out surveillance which is intrusive
- interception of communications

12.2 At no time should the Council or any officers undertake any surveillance if it falls within any of these categories. If in doubt seek the advice of the SRO, AO or legal services as soon as practicable.

13. Authorisation Procedures

13.1 Authorising Officers/Designated Persons for directed surveillance and CHIS

Authorising Officers are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

13.2 It is the responsibility of Authorising Officers to ensure that when applying for authorisation the principles of necessity and proportionality (see 12.10 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.

13.3 A list of AO's is contained at **APPENDIX 2**. Any requests for amendments to the lists must be made in writing and sent to the SRO.

13.4 Schedule 1 of statutory instrument No. 521 (2010) prescribes the rank or position of authorising officers for the purposes of Section 30(1) of RIPA (covert surveillance and CHIS). For Local Authorities they prescribe a "Director, Head of Service, Service Manager or equivalent".

The term Director is not defined within the Act but in Walsall Council it has been determined that it would normally equate to the Executive Director, Director or a member of Corporate Management Team.

13.5 The SRO designates which officers can be AO's. Only these officers can authorise directed surveillance and the use of CHIS. All authorisations must follow the procedures set out in the Policy. AO's are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the SRO.

- 13.6 All forms that are used in the respect of RIPA applications, renewals, reviews or cancellations should be taken from the Home Office website.

<https://www.gov.uk/government/collections/ripa-forms--2>

13.7 **Authorisation of Covert Directed Surveillance and Use of a CHIS**

Whether by Council officers or external agencies engaged by the Council, RIPA applies to all covert directed surveillance and use of CHIS. Council officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant application form and forward it to the relevant authorising officer.

- 13.8 Directed surveillance and use of a CHIS can only be authorised if the authorising officer is satisfied that the activity is:-

- (a) in **accordance with the law** i.e. it must be in relation to matters that are statutory or administrative functions of the Council.
- (b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and there is a crime threshold for directed surveillance as described in paragraph 3.23 above; and
- (b) **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct, or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

- 13.9 Officers making a RIPA application should ask the following types of questions to help determine whether the use of RIPA is necessary and proportionate:

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate)
- how the activity to be authorised is expected to bring a benefit to the investigation
- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation

- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the ECHR
- what other reasonable methods of obtaining information have been considered and why they have been discounted
- Authorising officers/designated persons should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable.

13.10 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation. Collateral intrusion occurs when an officer undertaking covert surveillance on a subject observes or gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into account by the authorising officer/designated person, particularly when considering the proportionality of the surveillance.

13.11 Particular care must be taken in cases where confidential information is involved e.g. matters subject to legal privilege; confidential personal information; confidential journalistic material; confidential medical information; and matters relating to religious leaders and their followers. In cases where it is likely that confidential information will be acquired, officers must specifically refer this to Legal Services for advice.

13.12 The activity must be authorised before it takes place. At the time of authorisation the authorising officer must set a date for review of the authorisation and review it on that date.

13.13 A copy of the completed relevant application and authorisation form must be forwarded to the SRO within one week of the authorisation for example by e-mail as a scanned document. The SRO will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application.

14. The Magistrates Court

14.1 Following changes under the Protection of Freedoms Act 2012, there is an additional stage in the process for the investigatory activities of Directed Surveillance and CHIS. After the Authorisation form has been countersigned by the AO, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation. The role of the Magistrates Court is set out in section 32A RIPA.

14.2 This section provides that the authorisation shall not take effect until the Magistrates Court has made an order approving such authorisation. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate;
- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:
- arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA;
- the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied;
- The local authority application has been authorised by an authorising officer or designated person (as appropriate);
- The grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
 - 29(7)(a) (for CHIS),
 - 30(3) (for directed surveillance and CHIS)

14.3 In cases where there is collaborative working with another agency, for example, the Police, as part of a single investigation or operation, only one authorisation from one organisation is required. This should be made by the lead authority of that particular investigation. Duplication of authorisation does not affect the lawfulness of the investigation or operation, but could create an unnecessary administrative burden. Where the Council is not the lead authority in the circumstances, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.

14.4 It should be noted that only the initial authorisation and any renewal of the authorisation require magistrates' approval.

14.5 There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified.

15. The procedure for applying for directed surveillance or use of a CHIS.

- Applicant officer completes an application
- Authorisation is sought from the Authorising Officer
- Applicant officer creates court pack
- Applicant officer proceeds to court
- Applicant officer organises the directed surveillance or use of a CHIS to take place

- Applicant provides the SRO with updated paperwork relating to reviews, renewals or cancellations

At any stage and particularly for inexperienced staff or potentially contentious investigations advice from Legal Services ought to be sought.

16. Additional Requirements for Authorisation of a CHIS

16.1 A CHIS must only be authorised if the following arrangements are in place:

- there is a Council officer with day to day responsibility for dealing with the CHIS (CHIS handler) and a senior council officer with oversight of the use made of the CHIS (CHIS controller);
- a risk assessment has been undertaken to take account of the CHIS security and welfare;
- a Council officer is responsible for maintaining a record of the use made of the CHIS;
- any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating; and
- records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS

17. Urgent Authorisations

17.1 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrate, urgent oral authorisations are no longer available.

18. Review of Authorisations

18.1 AO's must make arrangements to periodically review any authorised RIPA activity.

18.2 Officers carrying out RIPA activity or external agencies engaged by the Council to carry out RIPA activity must periodically review it and report back to the authorising officer if there is any doubt as to whether it should continue. For Juvenile CHIS's, the Code of Practice stipulates that the authorisation should be reviewed on a monthly basis. Reviews should be recorded on the appropriate Home Office form.

18.3 A copy of the Council's notice of review of an authorisation must be sent to the SRO within one week of the review to enable the central record on RIPA to be authorised.

19 Renewal of Authorisations

- 19.1 If the AO considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained.

Renewed authorisations will normally be for a period of

1. up to 3 months for covert directed surveillance,
2. 12 months in the case of CHIS,
3. 4 months in the case of juvenile CHIS

Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation.

- 19.2 Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form. The reasoning for seeking renewal of a RIPA notice should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

- 19.3 All renewals will require an order of the Magistrates Court.

20 Cancellation of Authorisations

- 20.1 The person who granted or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance or CHIS authorisation is no longer meets the criteria for authorisation. Cancellations must be made on the appropriate form.

- 20.2 Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and all welfare matters are addressed.

- 20.3 A copy of the Council's notice of cancellation of an authorisation must be sent the SRO within one week of the cancellation to enable the central record on RIPA to be updated.

21. What happens if the surveillance has unexpected results?

- 21.1 Those carrying out the covert surveillance should inform the authorising officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation.

In some cases the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

22 Errors

- 22.1 Proper application of the RIPA provisions, and robust technical systems, should reduce the scope for making errors. At Walsall Council the SRO will undertake a regular review of errors and a written record will be made of each review.
- 22.2 An error may be reported if it is a “relevant error”. Under section 231(9) of the Investigatory Powers Act 2016, a relevant error is an error by a public authority in complying with any requirements that are imposed on it by an enactment, such as RIPA, which is subject to review by a Judicial Commissioner.
- 22.3 Examples of a relevant error include where surveillance or CHIS activity has taken place without lawful authorisation, and/or without adherence to the safeguards set out within the relevant statutory provisions or the relevant Home Office Codes of Practice.
- 22.4 Where a relevant error has been identified, the Council should notify the Investigatory Powers Commissioner (IPCO) as soon as reasonably practical, and no later than 10 working days (unless otherwise agreed by IPCO). The process for informing IPCO is set out in the relevant Home Office Codes of Practice.

23. Records of RIPA Authorisations

- 23.1 There will be a central record of RIPA authorisations which is maintained by the SRO. The central record will contain the following information:
- the type of authorisation
 - the date it was given
 - the name and position of the AO
 - the unique reference number of the investigation or operation
 - the title of the investigation or operation, including a brief description and names of the subjects, if known
 - the date of attending the magistrates court
 - the determining magistrate
 - the decision of the court
 - the date and time of that decision

- the dates of any reviews
- the date of any renewal
- the AO for the renewal
- judicial information relating to any renewal
- whether the activity is likely to result in obtaining confidential or privileged information
- whether the authorisation was granted by a person directly involved in the investigation
- the date the authorisation was cancelled

23.2 In addition, the following information will also be retained by the SRO in a central file:

- a copy of the application and authorisation along with any additional supporting documentation and any notification of approval given by the AO
- a record of the period over which the surveillance took place
- the frequency of reviews prescribed by the AO and a copy of the record of those reviews
- a copy of any renewal authorisation together with any supporting documentation
- the date and time when any instruction to cease surveillance was given by the AO
- the date and time when any other instruction was given by the AO
- a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace.
- The officer making the application will be responsible for making sure that copies the original papers are given to that person as soon as practicable after each document is signed.
- The central record and copies of documents shall be maintained for seven years and provided to the Investigatory Powers Commissioner on request.

24. Handling of Material and Safeguards

24.1 When surveillance is carried out, information about the subject of the surveillance will be obtained. This may include information which an officer has observed and recorded, written communications, records, photographic and video images. There may also be information gathered about other persons (collateral intrusion). All such information is referred to here as material.

As well as the legislation governing RIPA, due regard must also be given to data protection legislation and the Authority's policies thereunder to ensure that the handling of private information continues to be lawful, justified and strictly controlled and is subject to robust and effective safeguards.

24.2 Any breaches of the safeguards which are in place to protect material must be investigated. A record of the investigation, conclusion and corrective actions is to be made and reported to the IPCO. Where appropriate, the Information Commissioner must also be notified.

24.3 Material should only be copied, retained and disseminated to the minimum degree necessary for authorised purposes, namely:

- the material is, or is likely to become, necessary for any of the statutory purposes set out in the 2000, 1997 or 1994 Acts in relation to covert surveillance
- the material is necessary for carrying out the functions of the Authority
- the material is necessary for carrying out the functions of the IPC or the Investigatory Powers Tribunal
- the material is necessary for legal proceedings
- the material is necessary for the performance of the functions of any person by or under any enactment.

24.4 Material obtained may be used to further investigations where it is necessary and provided that the safeguards are followed.

25. Use of Material as Evidence

25.1 Material obtained may be used as evidence in criminal proceedings.

25.2 Ensuring the continuity and integrity of evidence is important and governed by other legislation. Material obtained as a result of covert surveillance is also subject to the disclosure rules of the Criminal Procedure and Investigations Act 1996 and its associated codes of practice. Particular attention needs to be paid to the requirement to disclose all material obtained during the course of an investigation which may be relevant to the investigation when making an application for RIPA and in carrying out and recording information during the course of surveillance.

26. Disseminating Material

- 26.1** It is necessary to share information internally within the Authority and with external organisations such as other local authorities, the police and oversight organisations. This must be limited to the minimum necessary for the authorised purposes of the investigation or functions of the relevant organisation. This includes restricting dissemination within the Authority to only those persons who have a bona fide need to know the information. The amount of material disclosed should be the minimum necessary, including where relevant providing only a summary of the material.
- 26.2** Where material is disseminated outside the organisation, similar provisions will apply. The restrictions on further dissemination should be explicitly outlined in writing including, where relevant, the need to obtain written permission before disseminating the material further.
- 26.3** Material should not be disseminated to bodies outside the UK without ensuring that they have appropriate safeguards in place. The AO should be consulted before material is disseminated to bodies outside the UK.

27. Copying Material

- 27.1** Material, including extracts and summaries of it should only be copied to the minimum extent necessary for the authorised purposes. This also applies to any record which refers to the covert surveillance and the identities of any person to whom the material related.

28. Storage of Material

- 28.1** All material, copies, summaries and extracts of it must be stored to ensure no persons can access it without the proper authority. It must be stored to minimise the risk of loss or theft. Any person handling the material must adhere to this requirement. Measures in place to protect the material include:
- physical security – storage to be in buildings, rooms and cupboards etc where access is restricted
 - IT security to restrict access – storage is to be on shared servers, networks, databases etc where access is restricted to only those persons who need access to enable the material to be processed; to further the investigation or authorised purpose or to fulfil the functions of the legislation or this policy.

29. Retention and Destruction of Material

- 29.1** Where material is retained for an authorised purpose, it will be retained in accordance with the relevant retention policy. E.g. where material is retained for a prosecution, it will be retained in accordance with the document retention policy for prosecutions.

The material, including and copies, extracts or summaries should then be destroyed in a secure manner at the end of that period. Where material is not retained for one of the authorised purposes, then it should be destroyed in a secure matter as soon as it the need for retaining it is no longer relevant.

30 Surveillance products

- 30.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.
- 30.2 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.
- 30.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use of covert surveillance to facilitate its use in other investigations.
- 30.4 Material obtained through the use of directed surveillance or CHIS containing personal information will be protected by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). In addition to the considerations above, material obtained must be used, stored and destroyed in compliance with any other legal requirements, including confidentiality, and the Council's Data Protection, Information Security and Records Management Policies available on the intranet at the Protecting Information pages.

31. Training & Advice and Departmental policies, procedures and codes of conduct

- 31.1 The SRO will arrange regular training on RIPA. All authorising officers; designated persons and investigating officers should attend at least one session every two years and further sessions as and when required. Training can be arranged on request and requests should be made to the SRO. In particular training should be requested for new starters within the Council who may be involved in relevant activities.
- 31.2 Where in practice, departments have any policy, procedures or codes of practice in relation to RIPA that are different from or in addition to this Code, they must immediately seek advice from the Legal Services or the SRO.

32. Complaints

- 32.1 Any person who believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the SRO.

They may also complain to the Investigatory Powers Tribunal at:
Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Or via the website

[The Investigatory Powers Tribunal – Contacting us and requesting information](#)

DRAFT

Appendix 1 Non RIPA Authorisations



**APPLICATION FOR AUTHORISATION TO CARRY OUT
DIRECTED SURVEILLANCE
THIS IS NOT A RIPA AUTHORISATION FORM
THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA
SURVEILLANCE**

| | |
|---|---|
| Public Authority <i>(including address)</i> | Walsall Council Civic Centre Darwall Street Walsall WS1 1TP |
|---|---|

| | | | |
|---|----------------|----------------------------------|--|
| Name of Applicant | | Unit/Branch/ Division | |
| Full address | | | |
| Contact Details | Address Tel | | |
| Investigation/Operation Name (if applicable) | | | |
| Investigating Officer (if a person other than the applicant) | | | |

| |
|--|
| DETAILS OF APPLICATION |
| 1. Give rank or position of authorising officer |
| Has a pre-surveillance risk assessment been carried out? Yes <input type="checkbox"/> No <input type="checkbox"/> |
| 2. Describe the purpose of the specific operation or investigation. |
| |

| |
|--|
| |
|--|

| |
|---|
| 3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used. |
| |

| |
|---|
| 4. The identities, where known, of those to be subject of the directed surveillance. |
| |

| |
|--|
| 5. Explain the information that it is desired to obtain as a result of the directed surveillance. |
| |

| |
|--|
| 6. Identify <u>why</u> surveillance is necessary in this particular case: |
| |

| |
|---|
| 7. Explain <u>why</u> this directed surveillance is necessary in this particular case: |
| |

| |
|---|
| 8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion. |
| |

| |
|--|
| |
|--|

| |
|--|
| 10. Confidential Information. [Code paragraphs 3.1 to 3.12] INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION: |
| |

| | | | |
|--------------------------------|--|----------------|--|
| 11. Applicant's Details | | | |
| Name (Print) | | Tel No. | |
| Grade / Rank | | Date | |
| Signature | | | |

| |
|---|
| 9. Explain why this directed surveillance is proportionate to what it seeks to achieve. And why is this intrusion outweighed by the need for |
| 12. Authorising Officer's Statement [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] |
| surveillance in operational terms or can the evidence be obtained by any other means? |
| I hereby authorise as follows: |

| | | |
|---|--|--|
| Response | | |
| Initials | | |
| Why is authorised to conduct surveillance: | | |
| What is authorised for the surveillance: | | |
| Where is it to take place and for how long: | | |
| Why it is being authorised: | | |
| How will the surveillance be conducted: | | |

This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).

The Applicant and Authorised Officer will jointly review this authorisation on the date below to see whether authorisation should continue, be renewed or cancelled.

| |
|--|
| |
|--|

13. Authorised Officers statement explaining why in his / her view the directed surveillance is necessary and proportionate. This box must be completed and both aspects must be addressed.

| |
|--|
| |
|--|

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Home Office Codes of Practice relating to this issue.

| |
|--|
| |
|--|

Expiry of authorisation (3 months from the date / time of authorisation unless otherwise stated here)

| |
|--|
| |
|--|

Programme for subsequent reviews of this authorisation: Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

| |
|--|
| |
|--|

| | | | |
|---|--|----------------------|--|
| Authorising Officer Name (Print) | | Job Title | |
| Signature | | Date and time | |
| Expiry date and time [e.g. authorisation granted on 1 April 2005 – expires on 30 June 2005, 23.59] | | | |

| | | | | |
|--|--|----------------------|--|--|
| 15. Urgent Authorisation Authorising officer to explain why they considered the case so urgent that an oral instead of written authorisation was given. | | | | |
| | | | | |
| Name (Print) | | Job Title: | | |
| Signature | | Date and Time | | |
| Urgent authorisation Expiry date: | | Expiry time: | | |
| <i>Remember the 72 hour rule for urgent authorities</i> | e.g. authorisation granted at 5pm on June 1 st expires 4.59 on 4 th June | | | |

A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR REFUSED, MUST BE HELD ON THE INVESTIGATING OFFICER'S FILE

THERE IS NO REQUIREMENT TO PLACE A COPY OF THE AUTHORISATION ON THE CORPORATE DATABASE

Review of a Directed Surveillance authorisation

**REVIEW OF DIRECTED SURVEILLANCE AUTHORISAION
THIS IS NOT A RIPA REVIEW FORM
THIS FORM SHOULD NOT BE USED FOR REVIEWING RIPA
SURVEILLANCE**

| | |
|---|--|
| Public Authority <i>(including address)</i> | |
|---|--|

| | | | |
|--|--|---|--|
| Applicant | | Unit/Branch/ Division | |
| Full address | | | |
| Contact Details | | | |
| Operation Name | | Operation Number* *Filing Ref | |
| Date of authorisation or last renewal | | Expiry date of authorisation or last renewal | |
| Review Number | | | |

Details of review:

| 1. Review number and dates of any previous reviews. | |
|--|-------------|
| Review Number | Date |
| | |

| | |
|--|--|
| | |
|--|--|

2. Summary of the investigation / operation to date, including what private information has been obtained and the value of the information so far obtained.

| |
|--|
| |
|--|

3. Detail the reasons why it is necessary to continue with the directed surveillance.

| |
|--|
| |
|--|

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

| |
|--|
| |
|--|

5. Detail any incident of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

| |
|--|
| |
|--|

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

| |
|--|
| |
|--|

| |
|--|
| |
|--|

| 7. Applicant's Details | | | |
|------------------------|--|---------|--|
| Name (Print) | | Tel No. | |
| Job Title | | Date | |
| Signature | | | |

| 8. Review Officer's Comments, including whether or not the directed surveillance should continue. |
|---|
| |

| 9. Authorising Officer's Statement | |
|--|-----------|
| <p>I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue until its next [until its next review/renewal] [should be cancelled immediately].</p> | |
| Name (Print) | Job Title |
| Signature | Date |

| | |
|--------------------------|--|
| 10. Date of next review. | |
|--------------------------|--|

**A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR
REFUSED, MUST BE HELD ON THE INVESTIGATING
OFFICER'S FILE**

**THERE IS NO REQUIREMENT TO PLACE A COPY OF THE
AUTHORISATION ON THE CORPORATE DATABASE**



APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE

(PLEASE ATTACH A COPY OF THE ORIGINAL AUTHORISATION)

THIS IS NOT A RIPA RENEWAL FORM

THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA RENEWALS

| | | | |
|---|--|----------------------------------|--|
| Public Authority (including address) | | | |
| Name of Applicant | | Unit/Branch/ Division | |
| Full address | | | |
| Contact Details | | | |
| Investigation/Operation Name (if applicable) | | | |
| Renewal Number | | | |

Details of renewal:

| 1. Renewal numbers and dates of any previous renewals. | |
|--|------|
| Renewal Number | Date |
| | |

| | |
|--|--|
| | |
|--|--|

| |
|---|
| 2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of renewal. |
| |

| |
|--|
| 3. Detail the reasons why it is necessary to continue with the directed surveillance. |
| |

| |
|--|
| 4. Detail why the directed surveillance is still proportionate to what it seeks to achieve. |
| |

| |
|---|
| 5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance. |
| |

| |
|--|
| 6. Give details of the regular reviews of the investigation or operation. |
| |

| |
|--|
| |
|--|

| 7. Applicant's Details | | | |
|------------------------|--|----------------|--|
| Name (Print) | | Tel No. | |
| Grade / Rank | | Date | |
| Signature | | | |

| 8. Authorising Officer's Comments. <u>This box must be completed.</u> |
|---|
| |

| 9. Authorising Officer's Statement | |
|---|------------------|
| <p>I, [insert name], hereby authorise renewal of the directed surveillance/operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing.</p> <p>This authorisation will be reviewed frequently to assess the need for the authorisation to continue.</p> | |
| Name (Print) | Job Title |
| Signature | Date |

| | | |
|----------------------|--------------|--------------|
| | | |
| Renewal From: | Time: | Date: |

| | |
|---|--|
| Date of first review. | |
| Date of subsequent reviews for this authorisation. | |

A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR REFUSED, MUST BE HELD ON THE INVESTIGATING OFFICER'S FILE

THERE IS NO REQUIREMENT TO PLACE A COPY OF THE AUTHORISATION ON THE CORPORATE DATABASE



**CANCELLATION OF A DIRECTED
SURVEILLANCE AUTHORISATION
THIS IS NOT A RIPA AUTHORISATION FORM
THIS FORM SHOULD NOT BE USED FOR
AUTHORISING RIPA SURVEILLANCE**

| | |
|--|--|
| Public Authority (including full address) | |
| Name of Applicant Full Address Contact Details Investigation/Operation Name (if applicable) | |

Details of cancellation:

| |
|--|
| 1. Explain the reason(s) for the cancellation of the authorisation: |
| |

| |
|--|
| |
|--|

2. Explain the value of surveillance in the operation:

| |
|--|
| |
|--|

3. Authorising Officer's statement:

I [insert name], hereby authorise the cancellation of the directed surveillance/operation as detailed above.

Name (Print)**Job Title****Signature****Date****4. Time and Date of when the authorising officer instructed the surveillance to cease:**

| | | | |
|--------------|--|--------------|--|
| Date: | | Time: | |
|--------------|--|--------------|--|

5. Authorisation cancelled.**Date:****Time:**

**A COPY OF THIS FORM, ONCE IT HAS BEEN
AUTHORISED OR REFUSED, MUST BE HELD ON THE
INVESTIGATING OFFICER'S FILE**

**THERE IS NO REQUIREMENT TO PLACE A COPY OF
THE AUTHORISATION ON THE CORPORATE
DATABASE**

APPENDIX 2 List of Authorised Officer Posts for Authorising Directed Surveillance

| Post & Post Holder | Scope of Authorisation |
|--|--|
| Tony Cox Head of Law | Applications for miscellaneous and any application in an urgent situation or absence of primary authorising officer as listed below Applications pertaining to a non-criminal investigation into the conduct of an employee (non RIPA) |
| Director of Resilient Communities | Applications from Resilient Communities – where the council is the lead agency Applications for covert human intelligence source (CHIS) except in the case of juvenile / vulnerable adults in which case Annex A of the relevant Home Office Codes of Practice apply. |
| Elise Hopkins System Leader My Money My Home My Job | Applications from My Money My Home My Job |

In the absence of any post holder, this function is delegated to another trained AO, not to a person acting for the post holder.

Appendix 3 Legislation

The Regulation of Investigatory Powers Act 2000

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

The Protection of Freedoms Act 2012

<http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted>

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500

<http://www.legislation.gov.uk/uksi/2012/1500/made>

The Human Rights Act 1998

<http://www.legislation.gov.uk/ukpga/1998/42/contents>

The Data Retention and Acquisition Regulations 2018

<http://www.legislation.gov.uk/uksi/2018/1123/contents/made>

Home Office Revised Code of Practice on Covert Surveillance and Property Interference August 2018

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Home Office Revised Code of Practice on Covert Human Intelligence Sources August 2018

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf



Walsall Council

Investigatory Powers Act 2016

Acquisition of Communications Data Policy and Procedure

Page left intentionally blank

Contents

| | | |
|------|---|----|
| | Glossary | 3 |
| 1 | Policy Statement | 4 |
| 2 | Overview of IPA 2016 | 4 |
| 3 | Communications Data | 5 |
| 4 | Data that Cannot be Requested under IPA 2016 | 5 |
| 5 | Authorisations | 6 |
| 6 | Roles and responsibilities | 6 |
| 6.2 | Applicant and their responsibilities | 7 |
| 6.5 | Approval Officer (AO) and their responsibilities | 8 |
| 6.7 | Single point of contact (SPoC) and their responsibilities | 8 |
| 6.11 | Authorising Agency (OCDA) and their responsibilities | 9 |
| 6.12 | Senior Responsible Officer (SRO) and their responsibilities | 9 |
| 7 | Necessity Test | 10 |
| 8 | Proportionality Test | 10 |
| 9 | Authorised applications | 11 |
| 10 | Refused applications | 11 |
| 11 | Notices in pursuance of an authorisation | 12 |
| 12 | Duration of authorisations | 12 |
| 13 | Renewal of authorisations | 12 |
| 14 | Cancellation of authorisations | 13 |
| 15 | Offences for non-compliance with IPA 2016 | 13 |
| 16 | Monitoring and record keeping | 13 |
| 17 | Errors | 14 |
| 18 | Investigations resulting in criminal proceedings | 15 |

Glossary

| | |
|------|--|
| AO | Approval Officer |
| CPIA | Criminal Procedure and Investigations Act 1996 |
| IPA | Investigatory Powers Act 2016 |
| IPC | Investigatory Powers Commissioner |
| IPT | Investigatory Powers Tribunal |
| NAFN | National Anti-Fraud Network |
| OCDA | Office for Communications Data Authorisations |
| RIPA | Regulation of Investigatory Powers Act 2000 |
| SPoC | Single Point of Contact |
| SRO | Senior Responsible Officer. |

1. Policy Statement

- 1.1 Walsall Council will apply the principles of IPA 2016 and its relevant codes of practice when obtaining communication data. In doing so, the Council will also take into account its duties under other legislation, in particular the Human Rights Act 1998, Data Protection Act 2018 and its common law obligations.
- 1.2 The purpose of this policy is to ensure that:
- an individual's right to privacy is not unlawfully breached;
 - the investigation is necessary and proportionate to the alleged offence;
 - proper authorisations are obtained for obtaining of communications data;
 - the proper procedures are followed

2. Overview of IPA

- 2.1 The Investigatory Powers Act (IPA) 2016 regulates access to communications data. It requires local authorities to follow a specific procedure and obtain independent authorisation before obtaining communications data.
- 2.2 Failure to comply with IPA 2016 may mean that the Council's actions are unlawful and amount to a criminal offence. It may also mean that the evidence obtained would be inadmissible in court proceedings and jeopardise the outcome of such proceedings. Such action could also lead to a successful claim for damages against the Council.
- 2.3 It is in the public interest for criminal investigations to be undertaken efficiently and promptly. Therefore, where proportionate and necessary, the IPA should be used as a tool to advance criminal investigations accordingly.
- 2.4 This policy should be read in conjunction with the latest Home Office Code of Practice on Communications Data. Any queries or concerns in relation to the legalities of an investigation should be raised with Legal Services
- 2.5 This Policy should also be read in conjunction with Walsall Councils Regulation of Investigatory Powers Act 2000 Policy which deals with the use of surveillance and covert human intelligence sources (CHIS) and any relevant Enforcement Policy currently in force for the service undertaking the investigation.
- 2.6 Further information on IPA can be obtained from the Investigatory Powers Commissioner's Office, the body responsible for overseeing the use of investigatory powers.

3. Communications data

- 3.1 Communications data includes the who, when, where and how of a communication but not the content i.e. what was said or written. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning.
- 3.2 Communications data can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device.
- 3.3 It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.
- 3.4 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services including telecommunications or postal services.
- 3.5 Communications data is defined as entity data and/or events data.

Entity data is data about a person or thing (such as a device) or information Linking them, that can change over time. For example, information about which person is the account holder of email account and ‘who is the subscriber of phone number 01234 567 890?’

Events data concerns specific communications. For example, information about who sent a particular email or the location of a mobile phone when a call was made. There is a higher threshold to obtain events data than for entity data.

4. Data that cannot be requested under IPA 2016

- 4.1 Walsall Council does not have legal power under IPA 2016 to:
 - Intercept communications data;
 - Access the content of data communications e.g. the content of text messages, emails etc.;
 - Access internet connection records

5. Authorisations

5.1 It is crucial that the obtaining of communications data is properly authorised. No officer may seek to obtain any form of communication data unless they have obtained the proper authorisation to do so and that the authorisation is necessary for the purposes of detecting crime or of preventing disorder.

- An Approval Officer (AO) must be consulted.
- The application must be provided to the Single Point of Contact (SPOC)
- The application must be approved by the Office for Communications Data Authorisations (OCDA).

5.3 The following types of conduct may be authorised:

- conduct to acquire communications data - which may include Walsall Council obtaining communications data themselves or asking any person believed to be in possession of or capable of obtaining the communications data to obtain and disclose it; and/or
- the giving of a notice – requiring a telecommunications operator to obtain and disclose the required data.

5.4 In the case of Walsall Council the obtaining of communications data will be facilitated through our membership of the National Anti-Fraud Network (NAFN), which provides a comprehensive single point of contact (SPoC) service.

5.5 It will be the responsibility of NAFN to ensure all requests to a telecommunications/ postal operator for communications data, pursuant to the granting of an authorisation, comply with the requirements of the Code of Practice.

6. Roles and responsibilities

6.1 Obtaining communications data under the Act involves five roles:

- 1) Applicant;
- 2) Approvals Officer (AO);
- 3) Single Point of Contact (SPoC);
- 4) Authorising Agency (OCDA);
- 5) Senior Responsible Officer in a Public Authority (SRO)

6.2 **Applicant and their responsibilities**

The applicant is a person involved in conducting or assisting an investigation or operation and who makes an application in writing or electronically to obtain communications data. Applicants must submit applications through the central NAFN (SPoC) portal. Applicants will need to be registered with NAFN to access the portal and have valid login and security details. An allocated SPoC officer will then check all applications for legal compliance and, where necessary, provide feedback before submitting for authorisation to OCDA. The applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data.

- 6.3 Any member of staff engaged in a relevant role i.e. one which requires carrying out investigations may be an applicant, subject to any internal controls or restrictions put in place within public authorities.

The applicant must

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- include the operation name (if applicable) to which the application relates;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

- 6.4 The applicant should record subsequently whether the application was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

6.5 Approval Officer (AO) and their responsibilities

The Approval Officer is a person who is a manager at service level or above. The AO's role is to have an awareness of the application made by the Applicant and monitor the correct procedures are undertaken including contact with the SPoC.

- 6.6 The AO does not authorise or approve any element of the application and is not required to be operationally independent.

6.7 Single point of contact (SPoC) and their responsibilities

The SPoC is an individual trained to facilitate the lawful obtaining of communications data and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications and postal operators. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier.

- 6.9 Public authorities are expected to provide SPoC coverage for all reasonably expected instances of obtaining communications data. Walsall Council is a member of the National Anti-Fraud Network (NAFN). NAFN is an accredited body for the purpose of providing data and intelligence under the IPA for all public bodies. As part of their portfolio they offer a comprehensive SPoC service.

- 6.10 The SPoC will

- assess whether the acquisition of specific communications data from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data;
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators;
- engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations;
- advise on and manage the use of the request filter, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation;
- advise on the interpretation of the Act, particularly whether an authorisation is appropriate;

- provide assurance that authorisations are lawful under the Act and free from errors;
- consider and, where appropriate, provide advice on possible unintended consequences of the application;
- assess any cost and resource implications to both the public authority and the telecommunications operator or postal operator of communications data requirements.

6.11 Authorising Agency (OCDA) and their responsibilities

The Office for Communications Data Authorisations (OCDA) is the independent body responsible for the authorisation and assessment of all Data Communications applications under the Act and undertakes the following roles:

- Independent assessment of all Data Communications applications.
- Authorisation of any appropriate applications.
- Ensuring accountability of Authorities in the process and safeguarding standards.

6.12 Senior Responsible Officer (SRO) and their responsibilities

The Senior Responsible Officer (SRO) within Walsall Council is Simon Neilson the Executive Director Economy and Environment.

6.13 The SRO is responsible for:

- The integrity of the process in place within the public authority to obtain communications data;
- engagement with authorising officers in the Office for Communications Data Authorisations (where relevant);
- compliance with Part 3 of the Act and with the 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;
- ensuring the overall quality of applications submitted to OCDA;
- engagement with the IPC's inspectors during inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

7. Necessity test

- 7.1 Applications to obtain Communications Data should only be made where it is necessary for an applicable crime purpose.
- 7.2 This allows for applications to be made for entity data where the purpose of obtaining the data is for the prevention and detection of crime or prevention of disorder. This definition permits the obtaining of Entity data for any crime, irrespective of seriousness or for preventing disorder.
- 7.3 Applications for 'events data', previously referred to as service or traffic data, should only be made where the purpose is the prevention and detection of serious crime. Serious crime is defined in Section 86(2A) of IPA 2016, and includes, but is not limited to:
- Any crime that provides the potential for a prison sentence of imprisonment for 12 months or more (Either way or indictable offences);
 - Offences committed by a corporate body;
 - Any offence involving, as an integral part, the sending of a communication OR a breach of a person's privacy.
- 7.4 Necessity must be demonstrated by including in every application a short explanation of:
- The event under investigation, such as a crime.
 - The person whose data is sought, such as a suspect AND description of how they are linked to the event.
 - The communications data sought, such as a telephone number or IP address, and how this data is related to the person and event.
- 7.5 The application must explain the link between the three aspects to demonstrate it is necessary to obtain communications data.

8. Proportionality test

- 8.1 Applications should only be made where they are proportionate, and alternative means of obtaining the information are either, exhausted, not available or considered not practical to obtain the same information.
- 8.2 For example, the following should be considered:
- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
 - explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;

- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.
- An outline of how obtaining the data will benefit the investigation. The relevance of the data being sought should be explained and anything which might undermine the application.
- The relevance of time period requested
- How the level of intrusion is justified against any benefit the data will give to the investigation. This should include consideration of whether less intrusive investigations could be undertaken.
- A consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.
- Any details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion, if applicable.
- Where no collateral intrusion will occur, such as when applying for entity data, the absence of collateral intrusion should be noted. Any circumstances which give rise to significant collateral intrusion.
- Any possible unintended consequences. This is more likely in more complicated requests for events data or in applications for the data of those in professions with duties of confidentiality. E.G journalists/doctors/solicitors.

9. Authorised applications

- 9.1 Where the OCDA authorises the data request, this decision is communicated to the SPoC (NAFN) and actions are taken to request the data from the relevant telecommunications providers and other agencies holding such communications data to provide the necessary data.

10. Refused applications

- 10.1 Where the OCDA rejects an application, the Council has three options:
- Not proceed with the application;
 - Re-submit the application with revised justification and/or revised course of conduct to obtain the communications data; or
 - Re-submit the application without alteration and seek a review of the decision by the OCDA. This may only be done where the SRO (or a person of equivalent grade) has agreed to this course of action. The OCDA will provide guidance on this process.

11. Notices in pursuance of an authorisation

- 11.1 The giving of a notice is appropriate where a telecommunications operator or postal operator can retrieve or obtain specific data, and to disclose that data and the relevant authorisation has been granted. A notice may require a telecommunications operator or postal operator to obtain any communications data, if that data is not already in its possession.
- 11.2 For local authorities the role to issue notices to telecommunications/postal operators sits with the SPoC (NAFN), and it will be the SPoC's role to ensure notices are given in accordance with the Code of Practice.

12. Duration of authorisations

- 12.1 An authorisation becomes valid on the date the authorisation is granted by the OCDA. It remains valid for a maximum of one month. Any conduct authorised or notice served should be commenced/served within that month.
- 12.2 Any notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled.
- 12.3 All authorisations should relate to a specific date(s) or period(s), including start and end dates, and these should be clearly indicated in the authorisation.
- 12.4 Where the data to be obtained or disclosed is specified as 'current', the relevant date is the date on which the authorisation was granted.
- 12.5 Please note however that where a date or period cannot be specified other than for instance; 'the last transaction' or 'the most recent use of the service', it is still permitted to request the data for that unspecifiable period.
- 12.6 Where the request relates to specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date of authorisation.

13. Renewal of authorisations

- 13.1 A valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation and takes effect upon the expiry of the original authorisation. This may be appropriate where there is a continuing requirement to obtain data that may be generated in the future.
- 13.2 The Applicant will need to consider whether the application for renewal remains 'necessary and proportionate' and should reflect this in any renewal application made. The Authorising body (OCDA) will need to consider this carefully in authorising any renewal.

14. Cancellation of authorisations

- 14.1 Where it comes to the Council's attention after an authorisation has been granted that it is no longer necessary or proportionate, the Council is under a duty to notify the SPoC (NAFN) immediately.
- 14.2 It is the SPoC's (NAFN) responsibility to cease the authorised action and take steps to notify the telecommunications service provider. E.g. Such a scenario may occur where a legitimate application has been made for Entity data to identify and locate a suspect, but subsequently, and before the data has been obtained the Council becomes aware by some other legitimate means of the suspects name and address etc.

15. Offences for non-compliance with IPA 2016

- 15.1 It is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority (section 11 of IPA 2016).
- 15.2 The roles and responsibilities laid down for the SRO and SPoC are designed to prevent the knowing or reckless obtaining of communications by a public authority without lawful authorisation. Adherence to the requirements of the Act and this Code, including procedures detailed in this Policy, will mitigate the risk of any offence being committed.
- 15.3 An offence is not committed if the person obtaining the data can show that they acted in the reasonable belief that they had lawful authority.
- 15.4 It is not an offence to obtain communications data where it is made publicly or commercially available by a telecommunications/postal operator. In such circumstances, the consent of the operator provides the lawful authority. However, public authorities should not require, or invite, any operator to disclose communications data by relying on this exemption.

16. Monitoring and record keeping

- 16.1 Applications, authorisations, copies of notices, and records of the withdrawal and cancellation of authorisations, must be retained in written or electronic form for a minimum of 3 years and ideally 5 years. A record of the date and, when appropriate, the time each notice or authorisation is granted, renewed or cancelled.
- 16.2 Records kept must be held centrally by the SPoC and be available for inspection by the Investigatory Powers Commissioners Office upon request and retained to allow the Investigatory Powers Tribunal (IPT), to carry out its functions. The retention of documents service will be provided by NAFN.
- 16.3 The Team Leader Business Support will maintain an internal record on behalf of the SRO, and retain hard and electronic copies of all forms sent to NAFN.

- 16.4 The documents in the internal record are retained in accordance with Walsall Councils records management policy which complies with relevant data protection legislation. The original documents should be retained by the service area responsible for the surveillance activity.
- 16.5 The Investigatory Powers Commissioners Office (IPCO) monitors compliance with RIPA. Walsall's SRO will act as the first point of contact for the Inspectors within the Council, but all service areas that use IPA should expect to be involved in any inquiries from IPCO.
- 16.6 Nothing in the Code or this policy affects similar duties under the Criminal Procedure and Investigations Act 1996 requiring material which is obtained in the course of an investigation and which may be relevant to the investigation to be recorded, retained and revealed to the prosecutor.
- 16.7 For full details of the level of information expected to be retained by the SPoC reference should be made to the Code of Practice.
- 16.8 Regular reports will be made to Members in accordance with the requirements of the IPA Codes of Practice.

17. Errors

Errors generally

- 17.1 Where any error occurs in the granting of an authorisation or because of any authorised conduct a record should be kept.
- 17.2 Where the error results in communications data being obtained or disclosed incorrectly, a report must be made to the IPC by whoever is responsible for it. E.g. The telecommunications operator must report the error if it resulted from them disclosing data not requested, whereas if the error is because the public authority provided incorrect information, they must report the error. The SRO would be the appropriate person to make the report to the IPC.
- 17.3 Where an error has occurred before data has been obtained or disclosed incorrectly, a record will be maintained by the public authority (recordable error). These records must be available for inspection by the IPC.
- 17.4 A non-exhaustive list of reportable and recordable errors is provided in the Code of Practice.

Serious errors

- 17.5 There may be rare occasions when communications data is wrongly obtained or disclosed and this amounts to a 'serious error'. A serious error is anything that **'caused significant prejudice or harm to the person concerned'**. It is insufficient that there has been a breach of a person's human rights.

- 17.6 In these cases, the public authority which made the error, or established that the error had been made, must report the error to the Council's Senior Responsible Officer and the IPC.
- 17.7 When an error is reported to the IPC, the IPC may inform the affected individual subject of the data disclosure, who may make a complaint to the IPT. The IPC must be satisfied that the error is a serious error AND it is in the public interest for the individual concerned to be informed of the error.
- 17.8 Before deciding if the error is serious or not the IPC will accept submissions from the Public Authority regarding whether it is in the public interest to disclose. For instance, it may not be in the public interest to disclose if to do so would be prejudicial to the 'prevention and detection of crime'.

18. Investigations resulting in criminal proceedings

- 18.1 When communications data is been obtained during a criminal investigation that comes to trial an individual may be made aware data has been obtained.
- 18.2 If communications data is used to support the prosecution case it will appear in the 'served' material as evidence and a copy provided to the defendant.
- 18.3 Where communication data is not served but retained in unused material it is subject of the rules governing disclosure under the Criminal Procedure and Investigations Act 1996 (CPIA). The prosecution may reveal the existence of communications data to a defendant on a schedule of non-sensitive unused material, only if that data is relevant, and copies of the material may be provided to the defendant if it might reasonably be considered capable of undermining the prosecution case and/or assisting the defence.
- 18.4 Where communications data is obtained but not directly relied on to prove offences, the material may alternatively be listed in the 'Sensitive' unused material and not disclosed to the defendant. The CPIA sets out exemptions to the disclosure obligation. Under section 3(6) of that Act, data must not be disclosed if it is material, which, on application by the prosecutor, the Court concludes it is not in the public interest to disclose.
Any communications data, which comes within the scope of this exemption, cannot be disclosed. E.g. Material that reveals a 'method of investigation' is usually not disclosable.
- 18.5 If through any of the above notification processes, an individual suspects that their communications data has been wrongly obtained, the IPT provides a right of redress. An individual may make a complaint to the IPT without the individual knowing, or having to demonstrate, that any investigatory powers have been used against it.

Equality Impact Assessment (EqIA) for Policies, Procedures and Services

| | | | |
|--------------------------------|---|---|-------------|
| Proposal name | Regulation Of Investigatory Powers Act 2000 & Investigatory Powers Act 2016 Policies | | |
| Directorate | E&E | | |
| Service | Regulatory Services | | |
| Responsible Officer | David Elrington & Lorraine Boothman | | |
| Proposal planning start | 1 February 2020 | Proposal start date (due or actual date) | 20 May 2020 |

| | | | |
|----------|---|----------------------------------|-----------------------|
| 1 | What is the purpose of the proposal? | Yes / No | New / revision |
| | Show which category the proposal is and whether it is new or a revision. | | |
| | Policy | Yes | |
| | Procedure | No | |
| | Guidance | No | |
| | Is this a service to customers/staff/public? | No | |
| | If yes, is it contracted or commissioned? | No | |
| | Other - give details | It is to comply with Legislation | |
| 2 | What is the business case for this proposal? Please provide the main purpose of the service, intended outcomes and reasons for change? | | |
| | The policies are required to ensure that the Authority complies with the requirements set out in the Regulation Of Investigatory Powers Act 2000 & Investigatory Powers Act 2016. They are an update of a previous policy to implement changes in the legislation and incorporate feedback from the Commissioner's inspections. | | |
| 3 | Who is the proposal likely to affect? | | |
| | People in Walsall | Yes / No | Detail |
| | All | Y | |
| | Specific group/s | | |
| | Council employees | Y | |
| | Other (identify) | | |
| 4 | Please provide service data relating to this proposal on your customer's protected characteristics. | | |
| | The policy places requirements officers of the Council and the way in which it conducts surveillance and the acquisition of communications data. It ensures that such conduct is necessary and proportionate. It does not affect any particular groups. | | |
| | Walsall's population has risen by 6.2% from 253,401 in 2001 to 269,323 according to the 2011 census. The minority ethnic group population (everyone who is not White; English, Welsh, Scottish, Northern Irish or British) has shown an increase from 37,547 (14.81%) in 2001 to 62,085 (23.05%) in 2011. | | |



Compared with the rest of the West Midlands (33.98%), Walsall (23.05%) has a lower percentage of minority ethnic group people and is the fifth lowest, compared with the other West Midlands areas. However, it is clear that, with new communities emerging, this figure is likely see higher percentages in the 2021 census.

Walsall population by broad group 2001 to 2011

| Group | 2001 | 2011 |
|-----------------|-------------|-------------|
| White British | 85.2% | 76.9% |
| All other White | 1.2% | 1.9% |
| Mixed | 1.4% | 2.7% |
| Asian | 10.4% | 15.2% |
| Black | 1.4% | 2.3% |
| Other | 0.4% | 0.8% |

The largest increase is in people of Asian background, with a rise from 10.4% of all ethnic minority people in 2001 to 15.2% in 2011. Within this group, those of Pakistani background have increased the most to 5.3% of all residents (although Asian Indian remains the largest minority ethnic group at 6.1%).

Nine out of ten Walsall residents (90.1%) were born in the UK. There does not appear to be a high volume of residents from Eastern European countries living in the borough, with only 1.0% of residents, 2,681 people, born in EU Accession countries. This is in contrast with 2.0% in England and with neighbouring authorities of Wolverhampton (2.1%) and Sandwell (2.6%).

The Council is committed to meeting the needs and expectations of people who use its services. This means ensuring that services are delivered in a fair and legal way, ensuring that the residents and businesses of Walsall are treated with dignity and respect. All groups of customers will positively benefit from this regime. The people who will be subject to the use of these powers are those suspected of committing offences. The legislative regime ensures that due consideration is given to the risks of collateral intrusion.

| 5 | Please provide details of all engagement and consultation undertaken for this proposal. (Please use a separate box for each engagement/consultation). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---|-------------------|--|-------------------|------------------------|--------------------|--------------------------|------------|--|-------------|--------------|------------|-----------------------------------|--|--------------|--|--|-----------------------|--------------|--|--|-------------------|-----------------|------------|-----------------------------------|---------------------|-------------|------------|-----------------------------------|--|--------------|--|--|---|---|------------|------------------------------|------------------|--------------|--|--|--|--|
| | <p>Consultation has taken place with internal services - Finance, Human Resources, Legal Services, Public Health, Communications, Equalities team and the Councils Consultation Officer in order to reassure decision makers that the content of the report and the policies are correct and meet the requirements of Council Policy making. As these are statutory policies setting out controls and requirements on how officers conduct their investigations and use powers available to them and not the provision of a service and as the public cannot influence the contents of the policy, public consultation is not necessary.</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <table border="1"> <thead> <tr> <th>Officers</th><th>Consulted - Who</th><th>Date(s) consulted</th><th>Comments of consultees</th></tr> </thead> <tbody> <tr> <td>(a) Legal services</td><td>Mark Kelly Paul Green</td><td>05/06/2020</td><td>No comments on final report. Consulted previously in drafting of policy</td></tr> <tr> <td>(b) Finance</td><td>Jayesh Patel</td><td>05/06/2020</td><td>No comments made on final report.</td></tr> <tr> <td>(c) Procurement – for all procurement and contract related reports</td><td>Not required</td><td></td><td></td></tr> <tr> <td>(d) Property services</td><td>Not required</td><td></td><td></td></tr> <tr> <td>(e) Public health</td><td>Stephen Gunther</td><td>05/06/2020</td><td>No comments made on final report.</td></tr> <tr> <td>(f) Human resources</td><td>Emma Rogers</td><td>05/06/2020</td><td>No comments made on final report.</td></tr> <tr> <td>(g) Heads of other relevant service(s)</td><td>Not required</td><td></td><td></td></tr> <tr> <td>(h) Communications communications@walsall.gov.uk</td><td>Please insert name of officer reviewing</td><td>05/06/2020</td><td>To review at agenda planning</td></tr> <tr> <td>(I) Trade Unions</td><td>Not required</td><td></td><td></td></tr> </tbody> </table> | Officers | Consulted - Who | Date(s) consulted | Comments of consultees | (a) Legal services | Mark Kelly Paul Green | 05/06/2020 | No comments on final report. Consulted previously in drafting of policy | (b) Finance | Jayesh Patel | 05/06/2020 | No comments made on final report. | (c) Procurement – for all procurement and contract related reports | Not required | | | (d) Property services | Not required | | | (e) Public health | Stephen Gunther | 05/06/2020 | No comments made on final report. | (f) Human resources | Emma Rogers | 05/06/2020 | No comments made on final report. | (g) Heads of other relevant service(s) | Not required | | | (h) Communications communications@walsall.gov.uk | Please insert name of officer reviewing | 05/06/2020 | To review at agenda planning | (I) Trade Unions | Not required | | | | |
| Officers | Consulted - Who | Date(s) consulted | Comments of consultees | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (a) Legal services | Mark Kelly Paul Green | 05/06/2020 | No comments on final report. Consulted previously in drafting of policy | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (b) Finance | Jayesh Patel | 05/06/2020 | No comments made on final report. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (c) Procurement – for all procurement and contract related reports | Not required | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (d) Property services | Not required | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (e) Public health | Stephen Gunther | 05/06/2020 | No comments made on final report. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (f) Human resources | Emma Rogers | 05/06/2020 | No comments made on final report. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (g) Heads of other relevant service(s) | Not required | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (h) Communications communications@walsall.gov.uk | Please insert name of officer reviewing | 05/06/2020 | To review at agenda planning | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (I) Trade Unions | Not required | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | |
|---|---|---|---------------|-----------------------------------|
| 6 | Consultation Activity Internal Consultation as per the cabinet report process, in particular with legal services. | | | |
| | Concise overview of all evidence, engagement and consultation | | | |
| | Legal services involved in drafting the policy. No other feedback received. | | | |
| 7 | How may the proposal affect each protected characteristic or group? The effect may be positive, negative, neutral or not known. Give reasons and if action is needed. | | | |
| | Characteristic | Affect | Reason | Action needed Yes / No |
| | Age | None - The legislation stipulates that any conduct covered by the policies is necessary and proportionate. There are no impacts on protected characteristics. All impacts on the subject of surveillance and any potential collateral intrusion are outlined on each application. None None None None None None None None None None | | |
| | Disability | | | |
| | Gender reassignment | | | |
| | Marriage and civil partnership | | | |
| | Pregnancy and maternity | | | |
| | Race | | | |
| | Religion or belief | | | |
| | Sex | | | |
| | Sexual orientation | | | |
| | Other (give detail) | | | |
| | Further information | | | |

| | | | | |
|-----------------------------------|---|--|---------------------|--|
| 8 | Does your proposal link with other proposals to have a cumulative effect on particular equality groups? If yes, give details. | | | (Delete one) No |
| | | | | |
| 9 | Which justifiable action does the evidence, engagement and consultation feedback suggest you take? | | | |
| | A | No major change required | | |
| Action and monitoring plan | | | | |
| Action Date | Action | Responsibility | Outcome Date | Outcome |
| 15/07/2020 | Policies are considered at Cabinet | D Elrington, L Boothman, Paul Gordon, Simon Neilson. | 15/07/2020 | Policies will be approved to proceed to Council or not. |
| To be confirmed | Policies are considered at Council | Simon Neilson, Cllr Perry | To be confirmed | Policies will be approved or not. Delegation will be granted or not |
| | | | | |
| | | | | |

| | |
|---|---------------|
| Update to EqIA | |
| Date | Detail |
| | |
| | |
| Use this section for updates following the commencement of your proposal. | |

Contact us

Community, Equality and Cohesion
Resources and Transformation

Telephone 01922 655797

Textphone 01922 654000

Email equality@walsall.gov.uk

Inside Walsall: [http://int.walsall.gov.uk/Service information/Equality and diversity](http://int.walsall.gov.uk/Service_information/Equality_and_diversity)