FOR PUBLICATION

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

ANNUAL REPORT TO STANDARDS COMMITTEE 2019

MEETING:	**(1)**	**STANDARDS AND AUDIT COMMITTEE**
	(2)	**CABINET MEMBER FOR FINANCE AND GOVERNANCE**
DATE:	**(1)**	**24TH APRIL 2019**
	(2)	**tbc**
REPORT BY:		**RIPA SENIOR RESPONSIBLE OFFICER**
WARD:		**ALL**

FOR PUBLICATION

(Exempt information by virtue of Paragraph 1
of Part I of Schedule 12A of the Local Government Act 1972)

1.0 PURPOSE OF REPORT

1.1 To give an annual report to members on activities relating to surveillance by the Council and policies under the Regulation of Investigatory Powers Act 2011.

2.0 RECOMMENDATION

2.1 To note the report.

2.2 That the Surveillance Policy be updated as set out in this report with the Local Government and Regulatory Manager authorized to make any necessary consequential amendments.

10.3 That the proposed activity for 2019/20 be progressed.

3.0 BACKGROUND

3.1 **RIPA**

Chesterfield Borough Council has powers under the Regulation of Investigatory Powers Act 2000 (RIPA) to conduct authorised directed surveillances (DI) and use of human intelligence sources (CHIS) in certain circumstances in connection with the conduct of criminal investigations. These powers arise from the need to protect the rights of individuals relating to private and family life (including business relationships).

3.2 **Reporting to Members**

This report is submitted to members as a result of the requirement to report to members under paragraph 3.35 of the Home Office Code of Practice for Covert Surveillance and Property Interference. The previous report was submitted to members in April 2018. Further reports will continue to be submitted annually whether or not there has been any authorised surveillance.

3.3 **Background**

All directed surveillances (covert, but not intrusive) and use of covert human intelligence sources (CHIS) require authorisation by a senior Council officer and the exercise of the powers is subject to review. The controls are in place in accordance with

the Human Rights Act, particularly the right to respect for family and private life.

3.4 Originally the Office of the Surveillance Commissioner (OSC) oversaw the exercise by councils of their surveillance powers. However, since September 2017 and the coming into effect of the Investigatory Powers Act 2016 this role is undertaken by the Investigatory Powers Commissioner (IPC)[1]. The Right Honourable Sir Adrian Fulford is the IPC.

3.5 A confidential database of authorised surveillances is maintained, charting relevant details, reviews and cancellations. There have been no authorisations since 2010.

3.6 Substantial changes were made to the powers of Local Authorities to conduct directed surveillance and the use of human intelligence sources under the Protection of Freedoms Act 2012.

3.7 As from 1 November 2012 Local Authorities may only use their powers under the Regulation of Investigatory Powers Act 2000 to prevent or detect criminal offences punishable by a minimum term of 6 months in prison (or if related to underage sale of alcohol and tobacco – not relevant to this Council). The amendment to the 2000 Act came into force on 1 November 2012.

3.8 Examples of where authorisations could be sought are serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. The surveillance must also be necessary and proportionate. The 2012 changes mean that authorisations cannot be granted for directed surveillance for e.g. littering, dog control or fly posting.

[1] https://www.ipco.org.uk/

3.9 As from 1 November 2012 any RIPA surveillance which the Council wishes to authorise must be approved by an authorising officer at the council and also be approved by a Magistrate; where a Local Authority wishes to seek to carry out a directed surveillance or make use of a human intelligence source the Council must apply to a single Justice of the Peace.

3.10 The Home Office have issued guidance, in the form of codes of practices, to Local Authorities and to Magistrates on the approval process for RIPA authorisations. The latest code of practice guidance was issued in September 2018.[2] The changes in this latest guidance are considered later in this report.

4.0 Activity over 2018

No directed surveillance

4.1 During 2018 no directed surveillances (DS) or use of human intelligence sources (CHIS) were authorised by the Council under the Act. The police used Council CCTV for a duly authorised monitoring exercise, but as this was not a Council investigation RIPA was not engaged for this authority.

Training

4.2 In the 2018 annual report members were informed that an Aspire Learning module covering all key issues of RIPA had been trialled by some enforcement officers and was to be rolled out to all officers involved with enforcement, their managers, relevant legal officers and also the chief executive (who has ultimate responsibility). Further, more detailed, modular training would be considered as and when necessary in due course.

4.3 All of those officers identified as requiring training completed the mandatory RIPA module in 2018. This totalled 71 officers. A

[2] https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

100% completion rate is an excellent outcome, though 4 of these are not certified as successfully completing the module. However, they will be required to revisit the training module each year. A further three officers (whose work does not involve investigations) have voluntarily completed the training.

4.4 Last year it was reported that enquiries had been made of Arvato and Kier as to whether they use surveillance. Arvato does not use surveillance that requires authorisation under RIPA. Kier's function does not require the use of surveillance.

4.5 In addition to the RIPA module, the Monitoring Officer, who is the RIPA Senior Responsible Officer, has also undertaken an external training workshop about recent changes (January 2019) and has studied the 2018 guidance.

No inspection

4.6 No inspection of the Council's procedures, either in person or through a desktop exercise, has taken place by the Investigatory Powers Commissioner in the past year (the last inspection took place in March 2016).

Internal guidance

4.7 Intended guidance on the use of e.g. body cams by Council enforcement staff was not developed as intended. This will be carried forward to 2019, see below.

Governance

4.6 Since the Constitution update in 2017 the responsibility for the RIPA function is with the Cabinet Member for Finance and Governance.

5.0 OSC / IPC Inspections and Annual Reports

5.1 Members will remember that in March 2016 a surveillance inspector conducted a routine inspection of the Council's

procedures. At that stage surveillance authorities were inspected every few years. The prior inspection was in 2012 and before that in 2010.

5.2 The inspector in 2016, while noting that no authorised surveillance had taken place since 2010, recommended various changes to practices so the Council could maintain a "state of readiness" in case it ever needed to seek authorisation. The recommendations were set out in the report to this Committee in 2017 and put into effect.

5.3 For the inspection year 2016-2017 the Chief Surveillance Commissioner, Lord Judge, in his Annual Report decided that for non-unitary councils, where statutory powers have not been used at all, or very rarely during the previous 3 years, any inspection process should begin with a "desktop" examination of papers where necessary. Current indications are that the IPCO will continue with this approach, though a physical inspection at a neighbouring authority has been carried out recently.

5.4 The final OSC annual report was published in December 2017.[3] It identified that reduced resources and the new legislative burdens of the Protection of Freedoms Act 2012 had meant that investigations mostly now tended to be overt. However, local authorities should keep prepared to use the procedures and should guard against inadvertent use or misuse of the powers.

5.5 Social media was identified as a new medium where surveillance laws might be engaged and might require authorisation where repeated visits were made to the same material notwithstanding it was placed on public social media sites. An OSC open letter to local authorities in April 2017

[3] https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202016%20-%202017%20with%20new%20page%20furniture.pdf

stressed that lawful overt investigation of "open source" material could drift into covert surveillance falling within the legislation. The 2018 code of practice expands on this.

5.6 There has been no annual report issued by the IPC to date relating to local authority investigatory powers.

5.7 The codes of practice are admissible in court proceedings and may be taken into account by the IPC. Public authorities may be asked to justify their approaches against the codes.

6.0 Updated Guidance: 2018 Code of Practice

6.1 There are a number of changes contained in the 2018 updated guidance. The key ones are summarised below.

Social Media and the Internet

6.2 The availability of online information should be used by public authorities for their statutory purposes. While much material may be accessed without the need for a RIPA authorisation, persistent study of an individual's online presence or where material is to be extracted and recorded may engage privacy considerations, and RIPA authorisations may need to be considered. Just because material is easy to obtain does not mean it does not need authorisation.

6.3 Views of social media sites should only be where necessary and must be proportionate. Repeated viewing and/or recording will engage RIPA. Automatic internet search tools (for example, Google Alerts – where the internet is automatically monitored for new content according to saved search criteria) can also engage RIPA.

6.4 Use of the internet in itself can be seen as designed to be covert, as can Facebook friend requests or setting up fake profiles to gain access to information. Setting up a false identity

is not unlawful in itself but to do so may require authorisation. Using the identity of a person known, or likely to be known, to the subject of interest or users of an internet site without authorisation or consent of that person could also breach RIPA.

6.5 Establishing a relationship to obtain information without disclosing identity may involve deployment of CHIS (Covert Human Intelligence Sources). So care is needed as use of social medial or the CHIS relationship may now require authorisation and court approval. Enforcement action can be taken against local authorities for breaches.

6.6 Consideration should be given as to whether or not the individual knows surveillance is underway. Where a public authority has taken reasonable steps to inform individual that surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation may not normally be available.

6.7 While there may be reduced expectation of privacy on some internet platforms as the information is openly available within the public domain, the intention was not to make it available for covert investigative activity, regardless of privacy settings. However, publicly accessible databases (e.g. information about companies and directors on the Companies House website) are unlikely to require investigation authorisation. It will be a matter of fact and degree, and the code of practice gives detailed guidance to assist decisions. Regulation cannot be avoided by using third parties to carry out any searches.

6.8 Care should also be taken if there is collateral intrusion. Even though an individual may have consented for the public authority to access online material, consideration also needs to be taken of whether it contains private information relating to third parties who have not given consent, and whether authorisation is necessary. This would include individuals who

comment or post information on the accounts under surveillance.

6.9 Any actions must also comply with GDPR and Data Protection Act 2018, including the new law enforcement processing requirements for criminal investigations and prosecutions.

Employee Surveillance and Monitoring

6.10 While surveillance of employees is outside RIPA, any surveillance – or monitoring - involving employees must comply with Part 3 of the Employment Practices Code[4], and the Data Protection Act 2018. Monitoring is not only associated with disciplinary investigations, but also routine activities such as monitoring to ensure those working in hazardous environments are not put at risk due to unsafe working practices.

6.11 Where monitoring goes beyond one individual simply watching another and involved the manual or automatic recording/processing of personal data it must be done in a way that is lawful and fair to workers. Any adverse impact on workers must be justified by the benefits to the employer and others.

Use of Drones

6.12 Use of airborne crafts to carry out surveillance and now covered by the guidance. They can be regarded as covert due to their reduced visibility at altitude. Therefore the usual rules about directed surveillance authorisations apply.

Comment: While the Council does not currently use drones, this is something that services will need to be aware of in the event use commences in future.

---

[4] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Error and Other Reporting

6.13 There is a new responsibility to report errors to the IPC, with new duties on the Senior Responsible Officer to have oversight of reporting errors, identifying the cause of errors and implementation of the process to minimise repetition of errors.

6.14 Public authorities must put procedures in place to ensure compliance, including careful preparation and checking of authorisations, reducing the scope for making errors. Regular reviews of errors must be undertaken by a senior officer and a written record made of each review.

6.15 Any "relevant error" must be reported to the IPC in view of the significant consequences on an affected individual's rights. This would cover errors by a public authority in complying with the legislative provisions, including:

- Surveillance without lawful authority
- Failure to comply with safeguards in statute or the code of guidance
- (While not a "relevant error") Any authorisation obtained due to an error of person providing information, relied on in good faith by public authority

Errors must be reported as soon as reasonably practical and within 10 working days (or longer as agreed with IPC) after it has been established that an error has occurred. Procedures should allow for interim notification pending full facts being established.

6.16 The report should contain:

- Details of the error

- Reasons why the report has not been available within 10 working days (if applicable)
- Cause of the error
- The amount of surveillance carried out and material obtained
- Any unintended collateral intrusion
- Any analysis or action taken
- Whether material retained or destroyed
- Steps taken to prevent recurrence

The IPC has power to issue guidance on the format of error reports.

6.17 The IPC can inform the person affected by a serious error if in the public interest for them to be informed. A breach of their rights is not in itself sufficient to amount to a serious error. The public authority will be asked for their views before a decision is made. The person informed of the error will also be informed of their rights to apply to the Investigatory Powers Tribunal.

6.18 In addition all material obtained under authority of a covert surveillance authorisation (or property interference warrant) must be handled in line with the public authority's safeguards and breaches (including breaches of data protection requirements) reported to the IPC and also the Information Commissioner. Legally privileged items, identified as such by the public authority's legal advisor, must also be reported to the IPC.

Review of Procedures

6.19 Internal safeguards must be periodically reviewed by the public authority, and it should be considered whether more information about their internal arrangements put into the public domain.

6.20 There is expanded guidance on procedures relating to the use of material as evidence, reviewing authorisations, handling material, dissemination of information, copying, storage and destruction of material and confidential/privileged material.

Changes in the Role of Senior Responsible Officer

6.21 In addition to the new role relating to error reporting (see above) the SRO also has a new duty to ensure that all authorising officers are of an appropriate standard. These are in addition to the existing duties of the SRO.

7.0 Surveillance Policy

7.1 The Council's RIPA Policy is available on the Council's website and here. Various amendments and additions are necessary as the result of the new guidance. These are shown in Appendix 1. They particularly relate to:

- Social Media
- Role of Senior Responsible Officer
- Error reporting
- CCTV
- Drones

There are also other best practice updates.

8.0 Activity in the current year

8.1 Looking forward, the Council's procedures continue to be strengthened in the light of best practice and the guidance, while noting that corporately authorisation process is very rarely appropriate or necessary and has not been used since 2010. If there is further guidance from the IPC members will be updated.

9.2 The mandatory online training (though Aspire Learning) will be checked for relevant updates in accordance with the guidance and/or supplemented to take account of changes and monitored.

9.4 A RIPA update will be sent to relevant officers.

9.5 Updated information will be placed on the RIPA and other pages of the Council's intranet, particularly related to social media.

9.5 Relevant policy and guidance will be developed, including the use of body cams by Council enforcement staff. The growth in use of CCTV by different services, whilst overt surveillance, requires greater consistency across the authority and a corporate CCTV policy should be developed, including the use of body cams.

9.6 Activity and procedures reviewed, including mechanisms for identifying and communicating errors.

10.0 RECOMMENDATION

10.1 To note the report.

10.2 That the Surveillance Policy be updated as set out in this report, with the Local Government and Regulatory Manager authorized to make any necessary consequential amendments.

10.3 That the proposed activity for 2019/20 be progressed.

11.0 REASON FOR RECOMMENDATION

11.1 To enable the Council to operate the RIPA system effectively and as required by law and guidance.

GERARD ROGERS
RIPA SENIOR RESPONSIBLE OFFICER

Further information from Gerard Rogers, Monitoring Officer and Regulatory & Local Government Law Manager, Legal Services - Tel 345310 or gerard.rogers@chesterfield.gov.uk