South Lakeland District Council

Cabinet

Wednesday 24 June 2020

Regulation of Investigatory Powers Act 2000 Annual Review

Portfolio:	Councillor Eric Morrell, Customer and Commercial Service and People Portfolio Holder
Report from:	David Sykes, Director of Strategy, Innovation and Resources
Report Author:	Linda Fisher, Legal, Governance and Democracy Lead Specialist (Monitoring Officer)
Wards:	N/A
Forward Plan:	Not applicable

1.0 Expected Outcome

1.1 That the operation of the Council's surveillance policies and practices under the Regulation of Investigatory Powers Act 2000 ("RIPA") are reviewed.

2.0 Recommendation

It is recommended that Cabinet:

(1) Considers and notes the review of the operation of the Council's policies and procedures as regards RIPA for the year 2019/20

(2) Endorses the constitutional amendment to list David Sykes as Senior Information Risk Officer.

(3) Endorses the updates to job titles resulting from Customer Connect within the Council Guidance on Surveillance under RIPA.

3.0 Background and Proposals

3.1 Review of RIPA

3.1.1 This report is an annual review of the Council's operation of RIPA for the period between 1 April 2019 and 31 March 2020. During that period there have been no applications for any authorisation for Directed Surveillance or use of Covert Human Intelligence Source. At the date of this report there are no live authorisations or applications for authorisation. There have also been no non RIPA authorisation requests.

3.1.2 RIPA regulates covert investigations by a number of bodies, including local authorities. The legislation was introduced to ensure that individuals' rights are protected while also ensuring that public authorities have the powers they need to do the job effectively. The Council is included within the RIPA framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources and has adopted a Surveillance Policy.

3.1.3 RIPA requires that when the Council undertakes Covert Surveillance for the purposes of a specific investigation in a manner that is likely to lead to the obtaining of private information about a person, a specific internal authorisation is required from a designated council officer. The surveillance contemplated in these circumstances is defined as Directed Surveillance. RIPA requires that when the Council arranges for a person to form a relationship with another person for the covert purpose of obtaining and disclosing information about that other person, a specific internal authorisation is required from a designated council officer. The surveillance contemplated in these circumstances is defined as use of a Covert Human Intelligence Source.

3.1.4 Since 1 November 2012 the Protection of Freedoms Act 2012 has additionally required that authorisations for both Directed Surveillance and Covert Human Intelligence Sources need be approved by the Magistrates' Court before they take effect. In order to give such approval, the Magistrates have to be satisfied that:

- There were reasonable grounds for the Authorising Officer approving the application to believe that the Directed Surveillance or deployment of a Covert Human Intelligence Source was necessary and proportionate and that there remain reasonable grounds for believing so; and
- The Authorising Officer was of the correct seniority; and
- The granting of the authorisation was for the prescribed purpose of preventing or detecting crime.

3.1.5 The Investigatory Powers Act 2016 ('the Act'), which came into force on 30 December 2016 sets out how communications data can be obtained. Much of the Act is only relevant to local authorities in a peripheral way. Local authorities are not included in the Schedule 4 list of relevant public authorities that may obtain communications data and section 61 specifically excludes local authorities from being able to obtain internet connection records (ICRs). However, section 73 defines local authorities as a relevant public authority for the purposes of Part 3 of the Act and section 78 – 79 set out the circumstances in which local authority authorisation for obtaining communications data (other than ICRs) can be granted.

3.1.6 In order to obtain communications data, the following tests must be satisfied:

- It must be for the purpose of preventing or detecting crime or of preventing disorder;
- It must be for the purpose of preventing or detecting crime or of preventing disorder;
- The local authority must be part of a collaboration agreement that has been published and has been certified by the Secretary of State;
- The authorisation must be granted by a designated senior officer, which means a director, head of service, service manager, or equivalent or a higher person;
- It must be granted to an officer of a local authority that is either a 'supplying' or 'subscribing' authority under the collaboration agreement. (The Council have not entered into a collaboration agreement.);
- A person who is acting as the single point of contact must be consulted, unless the circumstances are exceptional, i.e. an imminent threat to life; and
- The conduct authorised must be proportionate to what is sought to be achieved and judicial approval from a justice of the peace obtained.

3.1.7 The Office of Surveillance Commissioners (OSC) advises that authorities should provide levels of training appropriate to the needs of users. The Council requires training should be undertaken once every two years. Relevant officers attended training in February 2019. The Council's procedures are available on the intranet and the Legal, Governance and Democracy Lead Specialist (Monitoring Officer) is

available to provide advice to officers on compliance with RIPA. Therefore it is considered that this frequency of training is appropriate.

3.1.8 The general rules applicable to employee surveillance as espoused by the DPA, the General Data Protection Regulation (GDPR) and the employment code will remain the same. The Council must demonstrate and record its general obligation of data protection by design and default as detailed under Chapter 4, Section 57 of the Data Protection Act 2018.

3.1.9 Impact assessments - One of the main recommendations is that employers should undertake an impact assessment before undertaking surveillance. This is best done in writing and should, among other things, consider whether the surveillance is necessary and proportionate.

3.1.10 Chapter 4 of the Data Protection Act 2018 and Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA) (also known as a Privacy Impact Assessment) as a tool, which can help data controllers (in this case employers) identify the most effective way to comply with GDPR obligations. A DPIA is required when the data processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. Employee monitoring is very likely to be considered as high-risk processing under article 35 requiring a DPIA.

3.1.11 Before doing a DPIA, the data protection officer's advice, must be sought as well as the views (if appropriate) of data subjects or their representatives. The views of the Information Commissioners Office (ICO) may also have to be sought. In all cases the data controller, in this case the Council, is obliged to retain a record of the DPIA which may be reviewed by the ICO at a later date in the event of an audit or investigation arising from the data controller's use of personal data.

3.1.12 Article 6 - lawfulness - All forms of processing of personal data (including employee surveillance) have to be lawful by reference to the conditions set out in article 6 of the GDPR (equivalent to Chapter 2, Section 8 of the Data Protection Act 2018). One of these conditions is consent. Consent is more difficult under the Data Protection Act 2018 and GDPR. This is especially so for employers conducting employee surveillance. Part 1, section 2(1)(a) of the Data Protection Act 2018 makes specific regard to the lawful and fair processing of personal data on the basis of the 'data subject's' consent or another specified basis.

3.1.13 Article 6 states that the legitimate interests condition shall not apply to processing carried out by public authorities in the performance of their tasks. Therefore the Council must consider the applicability of the legal obligation and public interest/official authority conditions (articles 6(1)(c) and 6(1)(e) respectively) as justification for the surveillance.

3.2 CCTV Policy

3.2.1 The Closed Circuit Television (CCTV) Policy provides clear guidelines on the Council's use of CCTV and to protect the organisation from allegations of misuse of the system and to protect staff and the public from any abuse of the CCTV system. The CCTV Policy was reviewed by the Council in 2019 as part of the Surveillance Camera Commissioner Self-Assessment. The purpose of the Self-Assessment was for the Council to satisfy itself that it meets the principles of the Surveillance Camera Code of Practice. A copy of the completed Self-Assessment is at Appendix 1.

3.2.2 In addition to the above, the Council reviewed the CCTV Policy as part of the Assurance Review of Data Protection Compliance in March 2020. The Council is satisfied that the current CCTV Policy meets the audit recommendations.

3.2.3 As part of the annual RIPA review, relevant officers have confirmed the CCTV Policy has been adhered to throughout the period 1 April 2019 to 31 March 2020.

3.3 Council Constitution

3.3.1 An amendment to the Council's Constitution is proposed to clarify the authorised officers. It is proposed that the Director of Strategy, Innovation and Resources is named as the Senior Information Risk Officer rather than the RIPA Monitoring Officer for to avoid any misunderstanding.

3.4 Council Guidance on Surveillance under RIPA ('RIPA Guidance')

3.4.1 Whilst reviewing the RIPA operations of the Council, the Council's RIPA Guidance has also been considered and reviewed.

3.4.2 It is noted that minor changes to the RIPA Guidance are required to reflect the changes to various job titles as a result of the Council's Customer Connect Programme and these will be made as a result of the RIPA review.

4.0 Consultation

4.1 Copies of the current guidance and relevant forms for RIPA are all placed on the Council's intranet and web site.

4.4 The Portfolio Holder has been consulted and is content with the review set out in this report.

5.0 Alternative Options

5.1 The review has been undertaken to comply with legislation and the report is presented for information and note. An alternative option is not presented.

6.0 Links to Council Priorities

6.1 The review links into the Council Plan vision of 'working together to make South Lakeland the best place to live, work and explore'.

7.0 Implications

Financial, Resources and Procurement

7.1 There are no financial implications arising from this report.

Human Resources

7.2 There are no human resources implications save for the need to ensure that appropriate staff and members are given sufficient training in this area of law and practice.

Legal

7.3 The legal implications are as set out in the report.

Health, Social, Economic and Environmental

7.4 Have you completed a Health, Social, Economic and Environmental Impact Assessment? No

7.5 If you have not completed an Impact Assessment, please explain your reasons: This report is considered to have a neutral impact on sustainability

Equality and Diversity

7.7 Have you completed an Equality Impact Analysis? No

7.8 If you have not completed an Impact Assessment, please explain your reasons: Obtaining authorisation protects the Council and its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention of Human Rights. Provided activities undertaken are reasonable and proportionate they

will not be in contravention of Human Rights legislation. The satisfaction of such tests should ensure no breach of the Equality Act 2010.

Risk

Risk	Consequence	Controls required
Failure to comply with the terms of the legislation	Criminal enforcement action by the Council would be at risk of failure due to challenges to the evidence.	Compliance with the legislation, training and regular reviews.
Failure to review and update policies following legislative changes	Council could fail to meet legal requirements	Ensure regular review and compliance with legislation

Contact Officers

Linda Fisher Tel 01539 793370 Email linda.fisher@southlakeland.gov.uk

Appendices Attached to this Report

Appendix 1 – Surveillance Camera Commissioner Self-Assessment

Background Documents Available

Name of Background document	Where it is available
Council Guidance on RIPA	https://www.southlakeland.gov.uk/media/1917/guidance-on-surveillance-under-ripa-2000.pdf

Tracking Information

Signed off by	Date sent
Legal Services	N/A
Section 151 Officer	04/04/2020
Monitoring Officer	N/A
CMT	04/06/2020

Circulated to	Date sent
Director	04/06/2020
Human Resources Manager	05/06/2020
Communications Team	05/06/2020
Leader	N/A
Committee Chairman	N/A
Portfolio Holder	05/06/2020
Ward Councillor(s)	N/A
Committee	N/A
Executive (Cabinet)	24/06/2020
Council	N/A