Surveillance and Implementation of RIPA within the PPP

Committee considering report:	Joint Public Protection Committee
Date of Committee:	15 December 2020
Report Author:	Paul Anstey

1 Purpose of the Report

1.1 The Joint Management Board (JMB) requested an update on the subject following external audits of the partner authorities by the Investigatory Powers Commissioner's Office (IPCO).

1.2 To follow up on feedback from senior officers across each of the 3 partners that this process (external audit) could be improved if there was a greater collective understanding of how officers in the PPP may use the methods and powers incorporated under the relevant legislation and associated policy.

1.3 To circulate information about body worn cameras and CCTV for enforcement purposes.

1.4 To highlight the work of the National Anti-Fraud Network and how it links to the PPP.

2 Recommendation

2.1 To note the information in the report.

3 Implications and Impact Assessment

Implication	Commentary
Financial:	None
Human Resource:	None
Legal:	Each partner LA must show compliance with the Regulation of Investigatory Powers Act 2000 and its associated guidance. IPCO monitor this compliance through external audits.

Risk Management:	The PPP monitor their compliance with RIPA through the Case Management Unit, in conjunction with oversight from the PPP Manager. Any specific risks are escalated to the Joint Management Board (JMB)			
Property:	None			
Policy:	RIPA Policy			
	Positive	**Neutral**	**Negative**	**Commentary**
Equalities Impact:				
A Are there any aspects of the proposed decision, including how it is delivered or accessed, that could impact on inequality?		X		
B Will the proposed decision have an impact upon the lives of people with protected characteristics, including employees and service users?		X		
Environmental Impact:		X		
Health Impact:		X		
ICT Impact:		X		
Digital Services Impact:		X		

Council Strategy Priorities:		X		
Core Business:	X			The content of the report helps ensure smooth operation of the service.
Data Impact:		X		
Consultation and Engagement:	Sean Murphy			

4 Executive Summary

The work of the PPP includes investigations which require the use people and equipment to gather information. Each partner is required to have its own policy to meet the legal requirements of the Regulation of Investigatory Powers Act 2000 (RIPA).

The PPP has been intimately involved with the external audits conducted by the Investigatory Powers Commissioner's Office (IPCO) across the 3 partner authorities.

Principally these audits have focussed on the levels of awareness, across each authority in total, of RIPA and in particular its application to the use of social media.

West Berkshire were audited in January 2019, Bracknell Forest and Wokingham in March 2019. This was followed up at Bracknell with a further visit in December 2019 and Wokingham were due to be included but unfortunately had to cancel at short notice. This visit is still to be re-scheduled with the Senior Responsible Officer (SRO) for Wokingham who is not employed within the PPP.

Feedback from IPCO was generally positive and this report highlights a range of practical scenarios where the RIPA policy has been applied.

5 Supporting Information

Introduction

5.2 Each partner has its own RIPA Policy (See **Appendix A** for an example) and IPCO recommend regular and ongoing oversight of the actual or potential use of these powers.

5.1 Each partner has its own Senior Responsible Officer (SRO):

- Kevin Gibbs – Bracknell Forest
- Sarah Clarke – West Berkshire

- Susan Parsonage - Wokingham

5.2 The SRO works closely with the PPP Manager (Sean Murphy) who assists all 3 partners in their understanding of how RIPA applies to both PPP and non-PPP officers when conducting investigations.

Background – What is in the RIPA Policy?

5.3 RIPA is an acronym for the Regulation of Investigatory Powers Act 2000. This Act was introduced to ensure that surveillance and certain other intelligence gathering complies with the European Convention on Human Rights ('The Convention'), importantly Article 8 which provides:

(a) Everyone has the right to respect for his private and family life, his home and his correspondence;

(b) There shall be no interference by any public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

5.4 Article 8 is a qualified right. If the right to respect for one's home, private and family life is interfered with it has to be proportionate and in accordance with the exceptions above.

5.5 Article 6 of The Convention is also applicable. This deals with the right of everyone to a fair and public hearing within a reasonable time by an independent tribunal. This can include the investigative process supporting that process.

5.6 Part II of RIPA provides a statutory framework that is compliant with The Convention when using surveillance techniques. It also introduces national standards that apply to the police and other law enforcement agencies. Local authorities are classified as law enforcement agencies as they are tasked to investigate certain crimes. For example the PPP could use it for:

(a) Trading standards offences (running from fraud to animal welfare offences);

(b) Noise nuisance; and

(c) Non-compliance with enforcement notices.

5.7 By virtue of Section 48(2) of RIPA, surveillance includes:

(a) Monitoring, observing, listening to persons, their movements, their conversations or their other activities or communications;

(b) Recording anything monitored, observed or listened to in the course of surveillance; and

(c) Surveillance by or with the assistance of a surveillance device.

5.8 IPCO produce an annual report, the latest being for 2018. It stated that there had been a marginal increase in the number of the directed surveillance applications across all local authorities from 2017, from 233 to 309.

5.9 The PPP has applied for 1 authorisation at the magistrates this year to monitor social media for unlicensed waste carrier activity.

When would the PPP need to use the RIPA Policy?

5.10 The most likely use would be when a camera/cctv is needed to get information or when a person is used to gain information secretly. This would be for online investigations and finding out about people's communications data e.g. telephone numbers and registered billing addresses.

5.11 The PPP carries out many investigations and in doing so might gather private information about a person. It is therefore very important that there is a clear authorisation process for investigations which balances the risks and benefits of any such investigation. All applications are signed off by the Magistrates.

5.12 It is key for that authorisation process that officers know the seriousness of the offences they are investigating and be sure that what they are doing is necessary and proportionate.

5.13 The training and policy on these issues is of paramount importance to ensure that any evidence collected can be effective. The PPP has a good record of evidence gathering and the Case Management Unit has been very successful in its use of such evidence.

5.14 The PPP keep a list of all equipment that can be used for surveillance

5.15 The PPP use the National Anti-Fraud Network (NAFN) who are an independent body to process all the communication data requests, this is considered best practice.

Social Network Sites

5.16 The PPP operates in an open way across multiple sites to encourage good trading practices i.e. it uses its branded logo and account details to interact with people and businesses – usually to encourage fair trading and good practice.

5.17 It can be effective, on some occasions, to monitor online behaviours and actions of people and businesses without identifying PPP officers. The RIPA Policy also applies in these circumstances.

5.18 It is not easy for officers to investigate matters where social networks are involved, particularly when users post their information publicly. The PPP always consider the sensitivity of the information they are looking for and it is important to remain true to the proportionality and necessity tests in any investigation. They ask questions like 'do we think the person knows they have posted that personal information?'

Body Worn Cameras (BWC) and CCTV

5.19 Most of the time PPP Officers would use BWC openly as part of an investigation e.g. when conducting a search/seizure visit.

5.20 The benefit of such equipment is to improve the evidential value and/or transparency in any encounter.

5.21 If the equipment is used it is very important to make sure that the recorded data is managed properly and in accordance with the Data Protection Act 2018.

5.22 This equipment will not be used in a secret way unless specific approval is given by the relevant SRO.

5.23 The RIPA Policy for each partner makes it clear that use of this equipment should be in line with the Surveillance camera code of practice (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf). The most relevant principles for the PPP are listed below:

- Principle 1 - Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

- Principle 2 - The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

- Principle 3 - There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

- Principle 4 - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

- Principle 5 - Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

- Principle 6 - No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

- Principle 7 - Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

- Principle 8 - Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

- Principle 9 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

- Principle 10 - There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

- Principle 11 - When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

- Principle 12 - Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

5.24 Most recently the PPP has used either BWC or CCTV for the following types of investigations:

- Execution of a warrant for a complex regional fraud investigation (BWC).
- Surveillance of a fly-tipping hotspot (CCTV).

IPCO Key Findings when auditing the PPP

5.25 It was acknowledged that, like many local authorities, the PPP uses RIPA powers in a very limited way. There was some improvements required in relation to oversight of post authorisation checks and record keeping but that officers involved in the process were highly professional and committed.

5.26 The Rt.Hon. Lord Justice Fulford wrote to West Berkshire's Chief Executive stating *'Your Council was found to have a clear and comprehensive RIPA policy and arrangements in place for refresher training for the relevant key officers in February 2019. This is reassuring.'*

5.27 The Rt.Hon. Sir Brian Leveson wrote to Bracknell Forest's Chief Executive stating *'It is reassuring to note that your Council, under the direction of Sean Murphy, has embarked on an extensive training programme since the inspection in March. This has been both classroom based and via an e-learning package which includes a pass or fail knowledge test.'*

PPP Scenarios requiring the use of the RIPA Policy

5.28 An operation was conducted to investigate the sale of counterfeit and unsafe goods on eBay. This required PPP officers to establish and maintain a relationship with traders online to make test purchases.

5.29 An operation was conducted to investigate a rogue car dealer. This required PPP officers to act as a potential customer.

5.30 An investigation into waste carriers was conducted using social media to establish whether they had the appropriate licences and reduce the incidence of fly tipping.

5.31 PPP Officers carry out alcohol test purchasing on a routine basis and whilst these do not require RIPA authorisation it is considered best practice to review each operation as if they did.

The use of the National Anti-Fraud Network (NAFN)

5.32 The PPP partners, along with many other local authorities up and down the country, are members of NAFN which works across government and police forces UK wide to promote collaboration, communication and effective information sharing on a not-for-profit basis.

5.33 The key elements of the NAFN service the PPP can access are:

- Investigatory Powers Act 2016, acquisition of **communications data service** (used only for the prevention and detection of crime)
- Authorised Officer Services including Prevention of Social Housing Fraud Act 2013 and Council Tax Reduction Scheme Regulations 2013
- Overnight service for DVLA current vehicle keeper details
- National Automatic Number Plate Recognition (Trading Standards Only)
- Direct access to TransUnion and Equifax providing instant retrieval of credit reports and bank account verification and validation; access to Experian Reports
- Sanction Information Database (National database holding all trading standards prosecutions, cautions and penalties)
- National Register for Refusals and Revocations (Database of all taxi and private hire license refusals and revocations)
- Intelligence Database

What is Communications Data and why is it needed?

5.34 Communications data is the who, where, when and how of a communication but not its content. It is a vital tool used to investigate crime, protect the public and safeguard national security.

5.35 It can include the address on an envelope, the time and duration of a communication, the telephone number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It can also include data relating to unsuccessful call attempts i.e. when the person being dialled does not answer the call, but where the network has been able to connect it successfully. It does not include data relating to an unconnected call i.e. when a call is placed, but the network is unable to carry it to its intended recipient. It covers electronic communications (not just voice telephony) and also includes postal services.

5.36 The Home Office produces a range of guidance on the subject (https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-

disclosure-of-communications-data) and officers of the PPP receive training to understand how to use it in the course of their investigations.

5.37 The PPP make applications to NAFN to get targeted communications data about people or businesses they believe may have committed an offence. There is a clear authorisation process that is overseen by managers in the PPP.

5.38 It is often the information that NAFN is able to produce that helps track down people who have defrauded residents in the PPP area.

6 Other options considered

6.1 n/a for information only.

7 Conclusion

7.1 The PPP has been able to assist on 3 external audits for each of the partner authorities, helping to improve the overall levels of awareness of RIPA. The PPP only uses its RIPA powers in a very limited way, but when it does it takes great care to do so properly and in accordance with the comprehensive regulatory framework.

7.2 The PPP has an excellent track record in conducting high quality investigations and the use of RIPA is key to that success.

8 Appendices

8.1 Appendix A – Example of a RIPA Policy

Subject to Call-In:

Yes: ☐ No: ☒

The item is due to be referred to Council for final approval	☐
Delays in implementation could have serious financial implications for the Council	☐
Delays in implementation could compromise the Council's position	☐
Considered or reviewed by Overview and Scrutiny Management Committee or associated Task Groups within preceding six months	☐
Item is Urgent Key Decision	☐
Report is to note only	☒

Wards affected: all

Officer details: Paul Anstey. Head of Public Protection and Culture