Oversight and Governance
Chief Executive's Department
Plymouth City Council
Ballard House
Plymouth PL1 3BJ

Please ask for Helen Rickman
T 01752 668000
E helen.rickman@plymouth.gov.uk
www.plymouth.gov.uk
Published 25 March 2022

AUDIT AND GOVERNANCE COMMITTEE – SUPPLEMENT PACK

Monday 28 March 2022
2.00 pm
Warspite Room, Council House

Members:
Councillor Dr Mahony, Chair
Councillor Lowry, Vice Chair
Councillors Bingley, Evans OBE, Laing and Shayer.
Independent Members: Mrs Annette Benny and Mr Ian Shipperley.

Please find enclosed supplementary information related to agenda items 6 and 11.

Tracey Lee
Chief Executive

Audit and Governance Committee

Audit and Governance Committee

Date of meeting:	28 March 2022
Title of Report:	**Audit Actions Review**
Lead Member:	Councillor Nick Kelly (Cabinet Member for Finance)
Lead Strategic Director:	Brendan Arnold (Service Director for Finance)
Author:	Carolyn Haynes (Financial Controller)
Contact Email:	carolyn.haynes@plymouth.gov.uk
Your Reference:	Finance/CH
Key Decision:	No
Confidentiality:	Part I - Official

Purpose of Report

To provide the Committee with an update on the tracking of Audit recommendations from Grant Thornton and Devon Audit Partnership.

Recommendations and Reasons

Members of the Audit and Governance Committee to note the content of the report.

Reason: To update members on audit recommendations.

Alternative options considered and rejected
None as the Committee agreed to receive an update of all audit recommendations.

Relevance to the Corporate Plan and/or the Plymouth Plan
The implementation of all agreed audit recommendations are fundamentally linked to delivering the priorities within the Council's Corporate Plan and assists with ensuring limited resources are allocated to priorities which will maximise the benefits to the residents of Plymouth.

Implications for the Medium Term Financial Plan and Resource Implications:

Delivery of the audit plan will assist the Council in delivering value for money services.

Carbon Footprint (Environmental) Implications:
No direct implications

Other Implications: e.g. Health and Safety, Risk Management, Child Poverty:
Implementation of agreed audit recommendations is an intrinsic element of the Council's overall corporate governance, risk management and internal control framework.

Appendices

Ref.	Title of Appendix	Exemption Paragraph Number (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
		1	**2**	**3**	**4**	**5**	**6**	**7**
A	Devon Audit Partnership Audit Recommendations							

Background papers:

Title of any background paper(s)	Exemption Paragraph Number (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
	1	**2**	**3**	**4**	**5**	**6**	**7**

Sign off:

Fin	djn.21.22.309	Leg	Ls/38309/AC/21/3/22	Mon Off		HR		Assets		Strat Proc	

Originating Senior Leadership Team member: Brendan Arnold

Please confirm the Strategic Director(s) has agreed the report? Yes

Date agreed: 17/03/2022

Cabinet Member approval: by Cllr Nick Kelly by email

Date approved: 17/03/2022

Audit Action Review

1. Introduction

1.1 Audit Committee has agreed to receive regular reports which set track the completion of agreed recommendations to improve controls and minimise exposure to risk. This will provide ongoing assurance to Senior Management and Members (Audit & Governance Committee) that scheduled actions are taking place. As previously reported the Council recognises and responds promptly and effectively to the independent assurance work completed by our external auditors, Grant Thornton (GT) and our internal auditors, Devon Audit Partnership (DAP).

1.2 There are no outstanding audit recommendations from GT and Appendix one provides an update on recommendations from DAP

Status of Internal Audit Recommendations January '22

The chart to the right provides an overall breakdown of progress made by management in implementing audit recommendations. The pie chart shows the figures in percentage format and the legend details the actual numbers.

Not all recommendations can be quickly and easily implemented with some having other, longer dependencies which have to be addressed, before the recommendation can be actioned.

In addition to the 64 recommendations showing as fully implemented, management responses received indicate that a further 23 recommendations are currently work in progress (partially implemented). See table 1 below for breakdown across audits.

Of the 26 recommendations not yet implemented, it should be noted that a number have target implementation dates in the future. Table 2 below provides a brief summary of all the recommendations which are now overdue (including those which have been partially implemented), based on the target date provided by management when the draft report was finalised.

Please note, it is a coincidence that the number of recommendations not yet implemented (Table 1) and the number of recommendations reported as past their target date (Table 2) are the same (27).

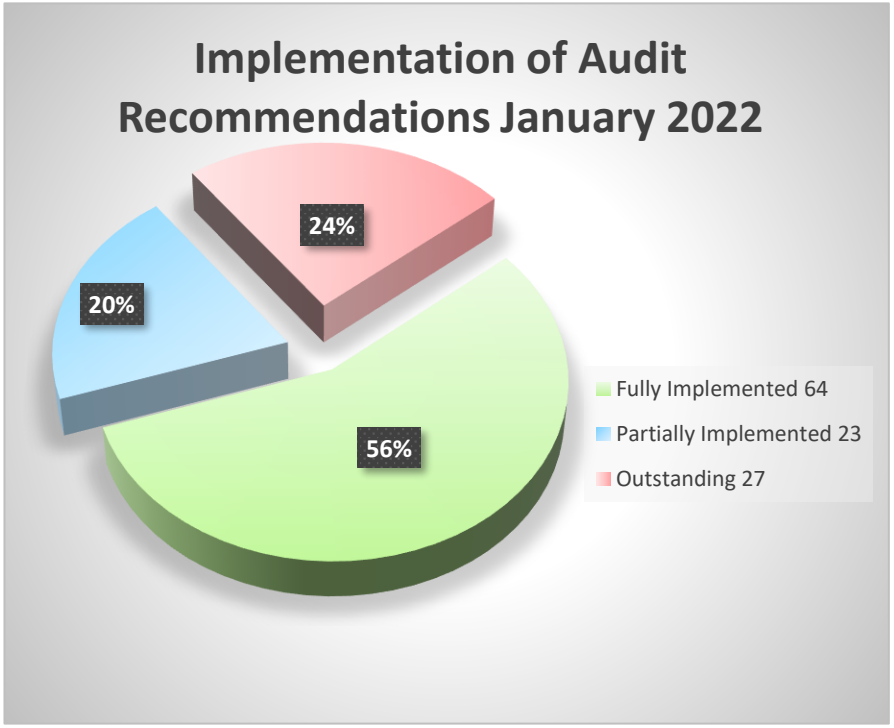

Table 1

Audits	Total Number of Recommendations	Fully Implemented	No Further Action	Partially Implemented	Not Yet Implemented
Council Tax	11	9		1	1
Creditors	6	4		2	
Sundry Debtors	9	5		3	1
Capital Programme	11	5			6
Purchasing Cards	11	7		2	2
Electoral Registration (Follow-Up)	4	3			1
Special Guardianship Orders	36	23		12	1
Street Lighting	14	8		3	3
Risk Management	3				3
CYPF Additional Spend	9				9
TOTAL	**114**	**64**		**23**	**27**

The audits listed below have been removed from Table 1 above as all High, Medium and Low recommendations have been actioned.

- Business Rates
- Housing Benefits
- Main Accounting System
- Treasury Management
- Empty Homes Scheme
- Information Asset Management
- Data Quality

Table 2

Audits	Overdue Recommendations	Summary Update
Council Tax	2	Not yet implemented due to pandemic and pressure on resources
Capital Programme	6	The review of the capital programme governance arrangements is underway, . The recommendations outstanding are all low priority.
Special Guardianship Orders	13	Nine recommendations are partially implemented with fulfilment reliant on introduction of revised operational procedures following an external review. Three are reliant on the Eclipse Project. One currently impacted by an ASC backlog.
Empty Homes Scheme	1	Work continues with the Portfolio Holder to develop Plan for Homes 4 with Empty Homes Plan being integral to it. These discussions will continue between now and May 2022.
Street Lighting	5	Two medium priority recommendations partially completed with one awaiting final completion of procedural manuals and pending restructure. Three medium or low relating to financial management procedures still to be addressed.
TOTAL	**27**	

Audit and Governance Committee

Date of meeting:	28 March 2022
Title of Report:	Surveillance, Covert Activities, and the Regulation of Investigatory Powers Act 2000 (RIPA)
Lead Strategic Director:	Andy Ralphs (Strategic Director of Customer and Corporate Services)
Author:	John Finch, Information Governance Manager
Contact Email:	John.Finch@plymouth.gov.uk
Your Reference:	RIPA Annual Report 2022
Key Decision:	No
Confidentiality:	Part I - Official

Purpose of Report
Surveillance is a tool that may be required for the Council to fulfil its obligations to investigate crime, prevent disorder, recover debt, protect the public and establish the facts about situations for which the Council has responsibility.

Staff may consider that it is appropriate to undertake covert activities that result in the subject of enquires being unaware that their actions are being monitored, or enquires are being undertaken without their knowledge. However, covert activities compromise an individual's 'right to privacy', so the use of a covert activity must be lawful, necessary and proportionate in order to comply with the Human Rights Act. Examples of the Council's use of covert surveillance are listed in Appendix A.

This report informs Members about the steps being taken to ensure that the Council is compliant in respect of covert activities.

Audit Committee are requested to accept the Surveillance and Covert Activities Policy.

Recommendations and Reasons
Council are required to be informed about the use of covert surveillance by staff when conducting investigations and to agree a policy.

Members are requested to acknowledge that covert activities can be a necessary and proportionate response for achieving the Council's objectives through approval of the Surveillance and Covert Activities Policy; which allows covert activities to be deployed where necessary and proportionate, under the control of a good practice process based on the Regulation of Investigatory Powers Act requirements.

The report informs members about covert surveillance that has taken place, changes to legislation since the last report and the steps being taken to ensure that the Council is compliant in respect of covert activities.

Alternative options considered and rejected

The alternative option is for Members to limit the option for Officers to use surveillance as an investigatory tool by:

a) deciding that Officers will not undertake surveillance or covert activities on behalf of the Council, or
b) Officers may only use covert activities when a serious crime is being investigated.

This option is rejected as the oversight Commissioners have not found Officers to be irresponsible, the Council has only initiated necessary investigations and has always been proportionate in its use of covert activities.

Thus Officers have been found to have the expertise to deploy the available powers appropriately and to now limit the use of surveillance would have a detrimental impact on Officers ability to undertake investigations in order to fulfil responsibilities of the Council.

Relevance to the Corporate Plan and/or the Plymouth Plan

This report is relevant to the Corporate Plan Values of being democratic, responsible and fair. Undertaking covert activities contributes to the corporate vision by reducing crime, helping to ensure residents feel safe, are happy and healthy and helping to ensure economic growth is not jeopardised through unfair or illegal activity.

Implications for the Medium Term Financial Plan and Resource Implications:
There are no significant implications for the medium term financial plan as the undertaking of surveillance and covert activities is a departmental casework related process. There is not a specific budget cost code and all costs are subsumed within service team budgets. Thus any equipment that is required is obtained through current budgets.

However in order to ensure compliance with the requirements of the HRA and other relevant legislation; sufficient trained managers and staff are required to be available and the resourcing of specialist staff role profiles must be incorporated into Directorate action plans.

Carbon Footprint (Environmental) Implications:
No implications.

Other Implications: e.g. Health and Safety, Risk Management, Child Poverty:
** When considering these proposals members have a responsibility to ensure they give due regard to the Council's duty to promote equality of opportunity, eliminate unlawful discrimination and promote good relations between people who share protected characteristics under the Equalities Act and those who do not.*

- Child Poverty - none.
- Community Safety - the purpose of the surveillance tool is to promote community safety, prevent crime and disorder, undertake fraud investigation and provide environmental protection.
- Health and Safety - in particular the use of CCTV can promote safety, but officers undertaking surveillance are potentially at risk.
- Risk Management - there is the possibility of loss of reputation and monetary penalties for the Council, through surveillance breaching privacy and that evidence obtained for an investigation will not be accepted. However, complying with RIPA prevents the Council breaching its obligations under the Human Rights Act and associated legislation; as well as enabling the product of surveillance to be used in accordance with the requirements of legislation and good practice.

Appendices
**Add rows as required to box below*

Ref.	Title of Appendix	Exemption Paragraph Number (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
		1	2	3	4	5	6	7
A	RIPA Policy							

Background papers:

**Add rows as required to box below*

Please list all unpublished, background papers relevant to the decision in the table below. Background papers are unpublished works, relied on to a material extent in preparing the report, which disclose facts or matters on which the report or an important part of the work is based.

Title of any background paper(s)	Exemption Paragraph Number (if applicable) *If some/all of the information is confidential, you must indicate why it is not for publication by virtue of Part 1of Schedule 12A of the Local Government Act 1972 by ticking the relevant box.*						
	1	2	3	4	5	6	7
Surveillance & Covert Activities Policy							

Sign off:

Fin	djn.21.22.319	Leg	402/NJ	Mon Off		HR		Assets		Strat Proc	

Originating Senior Leadership Team member: Andy Ralph (Strategic Director for Customer and Corporate Service)

Please confirm the Strategic Director(s) has agreed the report? Yes

Date agreed: 22/03/2022

This page is intentionally left blank

REGULATION OF INVESTIGATORY POWERS ACT 2000

Policy

Contents

1 Introduction

1.1 This document sets out the policy and procedures adopted by Plymouth City Council ("the council") in relation to Part II of the Regulation of Investigatory Powers Act 2000 ("RIPA"). The policy should be read in conjunction with the Home Office Codes of Practice on covert surveillance and covert human intelligence sources; acquisition and disclosure of communications data, and any guidance issued by the Investigatory Powers Commissioner's Office (IPCO).

1.2 The following terms are used throughout this Policy:

RIPA	Regulation of Investigatory Powers Act 2000
CHIS	Covert Human Intelligence Source
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
IPCO	Investigatory Powers Commissioner's Office
NAFN	National Anti-Fraud Network
CSP	Communications Service Provider

1.3 RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life. It should be noted that any use of activities under RIPA will be as a last resort and council policy is not to undertake such activities unless absolutely necessary.

2 Purpose and objectives

2.1 Directed surveillance, use of a CHIS or acquisition of communications data by or on behalf of the council must be carried out in accordance with this policy. Any such activity must be authorised by one of the Authorising Officers. All authorisations must then be approved by a Magistrate before any covert activity takes place. Staff directly employed by the council and any external agencies working for the council are subject to RIPA whilst they are working in a relevant investigatory capacity.

2.2 The purpose of the policy is to ensure the council is acting lawfully while undertaking its various enforcement functions, ensuring that directed surveillance, the use of a CHIS or acquisition of communication data is necessary and proportionate, and takes into account the rights of individuals under Article 8 of the Human Rights Act.

3 Roles and Responsibilities

3.1 Senior Responsible Officer (SRO):

3.1.1 The role of SRO will be undertaken by the council's Director for Customer and Corporate Services.

3.1.2 The SRO will be responsible for:

- The integrity of the process in place within the council for the management of CHIS and Directed Surveillance;
    - Ensuring that all authorising officers are of an appropriate standard;

- Compliance with Part 2 of the Act and with the Home Office Codes of Practice;
- Oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

3.2 Authorising Officers

3.2.1 The authorising officers shall be the only officers within the council who can authorise applications under RIPA in accordance with the procedures set out in section 7 of this policy.

3.2.2 Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers. Authorising Officers may not sub-delegate their powers in relation to RIPA to other officers.

3.2.3 The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

3.2.4 A list of Authorising Officers is listed on the Covert Surveillance staffroom page.

3.3 RIPA Monitoring Officer:

3.3.1 The RIPA Monitoring Officer shall have overall responsibility for the management and oversight of requests and authorisations under RIPA;

3.4 RIPA Administrator

3.4.1 The RIPA administrator shall

- issue a unique reference number to each authorisation requested under RIPA
- retain a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer maintain a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;
- review and monitor all forms and documents received to ensure compliance with the relevant law and guidance and this policy and procedures document in consultation with the RIPA Monitoring Officer and inform the Authorising Officer of any concerns;
- chase failures to submit documents and/or carry out reviews/cancellations;

3.5 Councillors:

3.5.1 The relevant Cabinet Portfolio holder will review the Councils use of RIPA on an annual basis.

4 Local Authority use of RIPA

4.1 RIPA limits local authorities to using three covert techniques, as set out below:

- Directed surveillance
- A Covert human intelligence source (CHIS) includes undercover officers, public informants and people who make test purchases (for enforcement purposes) in certain circumstances
- Communications data

4.2 Compliance with the provisions of RIPA, the Home Office Codes of Practice and this policy and procedures should protect the council, its officers and agencies working on its behalf against legal challenge. Section 27 of RIPA states that "conduct…shall be lawful for all purposes if an authorisation…confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation". If correct procedures are not followed, the council could be rendered liable to claims and the use of the information obtained may be disallowed in any subsequent legal proceedings.

4.3 Officers should be aware of the scope and extent of activities covered by the provisions of RIPA. In many cases investigations carried out by council officers will not be subject to RIPA, as they involve overt rather than covert surveillance

5 Directed Surveillance

Directed surveillance may only be authorised by the Council under RIPA for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco An explanation of terms used is set out below:

5.1 Surveillance for the purposes of the Act 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).
- Surveillance can be overt or covert.

5.2 Covert Surveillance

Covert Surveillance is surveillance carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is, or may be taking place.

5.3 Directed Surveillance

Directed Surveillance is surveillance which:

- is covert; and
- is not intrusive surveillance (see definition below - the council is prohibited by law from carrying out any intrusive surveillance);
- is not carried out as an immediate response to events where it would not be practicable to obtain authorisation under the Act;
- is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

5.4 Private information

Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. The way a person runs their business may also reveal information about his private life and the private lives of others. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact or associates with.

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 gathered may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate

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 direct surveillance authorisation is appropriate.

5.5 Overt Surveillance

5.5.1 Overt Surveillance will include most of the surveillance carried out by the council - there will be nothing secretive, clandestine or hidden about it. For example, signposted CCTV cameras normally amount to overt surveillance. In many cases, officers will be going about council business openly (e.g. a parking attendant patrolling a council car park).

5.5.2 However, care must be taken to ensure that officers are not intentionally acting as members of the public in order to disguise their true intent as this may then be considered as covert and require RIPA authorisation.

5.5.3 Similarly, surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

5.5.4 Overt surveillance does not require any authorisation under RIPA. Neither does low-level surveillance consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer

5.5.5 Although signposted CCTV cameras do not normally require authorisation, this will be required if the camera(s) are to be directed for a specific purpose which involves surveillance on a particular person.

5.5.6 Use of body worn cameras should be overt. Badges should be worn by officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary – for example, when issuing parking tickets.

5.6 Surveillance that is unforeseen and undertaken as an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation normally falls outside the definition of directed surveillance and therefore authorisation is not required. However, if a specific investigation or operation is subsequently to follow, authorisation must be obtained in the usual way before it can commence. In no circumstances will any covert surveillance operation be given backdated authorisation after it has commenced.

5.7 Directed surveillance will always be a last resort in an investigation, and use of a CHIS by the council is unlikely. These activities will only be undertaken where there is no other reasonable and less intrusive means of obtaining the information

5.8 Intrusive Surveillance

5.8.1 Intrusive Surveillance occurs when surveillance:

- is covert;
- relates to residential premises and/or private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

5.8.2 The Council will not undertake intrusive surveillance under any circumstances.

5.9 Social Networking Sites

The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

5.9.1 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert

Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

5.9.2 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

5.9.3 As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

5.9.4 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

5.9.5 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

6 Communications Data

6.1 Acquisition of Communications data is the 'who', 'when' and 'where' of a communication, but not the 'what' (ie the content of what was said or written). RIPA groups communications data into three types:

- Traffic data (which includes information about where the communications are made or received)
- Service use information (such as the type of communication, time sent and its duration); and
- Subscriber information (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services)

6.2 Under RIPA a local authority can only authorise the acquisition of the less intrusive types of communications data: service use and subscriber information. Under no circumstances can local authorities be authorised to obtain traffic data under RIPA.

6.3 Local authorities are not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

6.4 Council's Authorising Officers may not authorise the acquisition of communications data unless it is for the purpose of preventing or detecting a criminal offence and it meets certain conditions. This is known as the 'serious crime test'

6.5 What counts as a Serious Crime?

- An offence that is capable of attracting a prison sentence of 12 months or more
- An offence by a person who is not an individual (i.e. a corporate body)
- An offence falling within the definition of serious crime in section 81(3)(b) of the Act (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of person in pursuit of a common purpose)
- An offence which involves, as an integral part of it, the sending of a communication
- An offence which involves, as an integral part of it, a breach of a person's privacy

6.6 For access to communication data, a Single Point of Contact (SPoC) is required to undertake the practical facilitation with the communications service provider (CSP) in order to obtain the data requested. The SPoC must have received training specifically to facilitate lawful acquisition of communications data and effective cooperation between the local authority and CSP.

6.7 The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications to a Magistrate and a designated person in the authority is still required to scrutinise and approve any applications.

7 Covert Human Intelligence Source (CHIS)

7.1 A CHIS is defined as the use of an individual to create a relationship with a subject, for the purposes of obtaining information, where the purpose of the relationship is not disclosed to the subject. Interaction with the subject of surveillance is therefore required in order for an individual to be regarded as a CHIS. Activities of an undercover officer could fall within this definition. Additional careful monitoring and recording is required (see Home Office Code of Practice CHIS chapter 6).

7.2 The use of a CHIS, and their conduct, also requires authorisation under RIPA. It is considered unlikely that there will be any circumstances which would require the council to either use a CHIS or operate under cover and advice should be sought from the Senior Responsible Officer before any authorisation is applied for or granted. These provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating undercover. Great caution should be exercised in these circumstances.

7.3 The provisions of RIPA relating to CHIS do not apply where a situation would not normally require a relationship to be established for the covert purpose of obtaining information. For example:

- where members of the public volunteer information to the council as part of their normal civic duties;
- where the public contact telephone numbers set up by the council to receive information;

- where members of the public are asked to keep diaries of incidents in relation to, for example, planning enforcement, anti-social behaviour or noise nuisance. However, in certain circumstances, RIPA authorisation may be required if the criteria in section 26(2) of the Act are met.

8 Authorisation Procedures

8.1 Any directed surveillance, or the use of a CHIS undertaken by or on behalf of the council must be carried out in accordance with RIPA and must not commence until authorisation has been granted and has been approved by a relevant judicial authority. If such activities are undertaken without authorisation the RIPA Monitoring Officer or Senior Responsible Officer must be advised immediately. Only those officers employed in the designated Authorising Officer Posts can authorise an application under RIPA. Once authorised, the application must be presented to a Magistrate for final approval.

8.2 The acquisition of communications data can only be undertaken by a SPoC (although the same authorisation procedures will apply). If necessary the council would engage a third party to undertake this role.

8.3 Officers must discuss the need to undertake directed surveillance with their line manager before seeking an authorisation. All other reasonable and less intrusive options to gain the required information must be considered before an authorisation is applied for and the RIPA application must detail why these options have failed or have been considered not appropriate in the circumstances of the individual investigation.

8.4 All applications for authorisation must be made on the appropriate form. Guidance on completing the forms can be found on the council's intranet, together with a procedure for obtaining judicial approval. In the event of any query, officers making or authorising applications should consult the RIPA Monitoring Officer or the Senior Responsible Officer. The RIPA Monitoring Officer should be contacted prior to the completion of a RIPA application form so that a Unique Reference Number can be allocated.

8.5 Authorisations will not take effect until a Magistrate has made an order approving the grant of the authorisation. It is vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate

8.6 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. There is no requirement for the Magistrate to consider either cancellations or internal reviews.

8.7 In the unlikely event that officers find it necessary to seek authorisation for the use of a CHIS, additional safeguards must be considered and advice must first be sought from the RIPA Monitoring Officer or Senior Responsible Officer.

8.8 In any case where it is likely that confidential information may be acquired by directed surveillance or by the use or conduct of a source, the Authorised Officer who may grant authorisation is the Head of Paid Service or, in his/her absence, the person acting as Head of Paid Service.

8.9 Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual

welfare, or between a Member of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality may be involved

8.10 Covert surveillance of all legal consultations should be considered to be intrusive.

8.11 When considering an application, Authorising Officers must:

(a) have regard to the contents of this document, the training provided and any other guidance or advice given by the RIPA Monitoring Officer or the Senior Responsible Officer;

(b) satisfy his/herself that the RIPA authorisation will be:
- in accordance with the law;
- necessary in the circumstances of the particular case; and
- proportionate to what it seeks to achieve.

(c) assess whether or not the proposed surveillance is proportionate, considering the following elements:
- The custodial sentence applicable to the offence being investigated;
- 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 subject and others;
- Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all practical alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

(d) take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called 'collateral intrusion'), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible (the degree of likely collateral intrusion will also be relevant to assessing whether the proposed surveillance is proportionate);

(e) consider any issues which may arise in relation to the health and safety of council employees and agents, and ensure that a risk assessment has been undertaken if appropriate.

8.12 When authorising the conduct or use of a CHIS, the Authorising Officer must also:

(a) be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;

(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;

(c) consider the likely degree of intrusion for all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and

(e) ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

8.13 Authorising Officers should consult the RIPA Monitoring Officer or the Senior Responsible Officer before authorising the use of conduct of a CHIS to ensure that all legal requirements are complied with.

8.14 If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that date. Records must be kept in relation to all RIPA applications and authorisations in accordance with paragraph 13 below, and to facilitate this, each investigation or operation should be given a unique reference number (URN) on the application form by

the RIPA Monitoring Officer. Any subsequent forms (eg. renewals or cancellations) relating to the same investigation or operation should be identified by means of the same URN.

8.15 A flow chart for the authorising procedure can be found in Appendix A.

9 Urgent Authorisations

It is no longer possible for urgent authorisations to be given orally. However, a Magistrate may consider an authorisation out of hours in exceptional circumstances.

10 Duration of Authorisations

10.1 Authorisations will have effect until the date for expiry specified on the relevant form. They must be granted for the designated period of three months for directed surveillance, 12 months for the use or conduct of a CHIS and one month for the acquisition of communications data. No further operations should be carried out after the expiry of the relevant authorisation unless it has been renewed. It will be the responsibility of the officer in charge of an investigation to ensure that any directed surveillance or use of a CHIS is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. The RIPA Monitoring Officer will perform an auditing role in this respect but the primary responsibility rests with the officer in charge of the investigation.

10.1.1 An authorisation for the use or conduct of a juvenile CHIS is four months from the date the authorisation is given,

10.1.2 An authorisation where it is intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege is reduced from the usual 12 months to 6 months (in the case of an intelligence service authorisation), or 3 months (for any other public authority).

10.2 Authorisations should be reviewed at appropriate intervals in order to update the Authorising Officer on progress on the investigation and whether the authorisation is no longer required. Review periods should be set by the Authorising Officer, but should normally take place on a monthly basis unless the Authorising Officer considers that they should take place more or less frequently (if so, the reasons should be recorded). If the surveillance provides access to confidential information or involves collateral intrusion, there will be a particular need to review the authorisation frequently. The results of reviews should be recorded on the appropriate form.

10.3 Authorisations must be cancelled as soon as they are no longer necessary. Even if an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled. The responsibility for ensuring that authorisations are cancelled rests primarily with the officer in charge of the investigation, who should submit a request for cancellation on the appropriate form. However, if the Authorising Officer who authorised any directed surveillance or the use or conduct of a CHIS (or any Authorising Officer who has taken over their duties) is satisfied that it no longer meets the criteria upon which it was authorised, s/he must cancel it and record that fact in writing even in the absence of any request for cancellation.

10.4 If it is required, a renewal must be authorised prior to the expiry of the original authorisation. Applications for renewal should be made on the appropriate form shortly before the original

authorisation period is due to expire. Officers must take account of factors which may delay the renewal process (eg intervening weekends or the availability of the relevant authorising officer and a Magistrate to consider the application). The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. Renewals of an authorisation may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be cancelled and new authorisation sought. The renewal will begin on the day when the original authorisation would otherwise have expired.

11 Material Obtained During Investigations

11.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the council's policies and procedures currently in force relating to document retention. Advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer where appropriate.

11.2 Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the council, unless directed by any court order, should only be considered in exceptional circumstances, and in accordance with advice from the RIPA Monitoring Officer or the Senior Responsible Officer.

11.3 Where material obtained is of a confidential nature such as medical records or material covered by legal professional privilege then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;
- Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;
- Confidential material should be destroyed as soon possible after its use for the specified purpose.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer.

12 Assessment and Review

12.1 Following completion of any investigation/operation involving the use of RIPA, an assessment should be undertaken. This should detail the information obtained and how it was used to take the case forward.

12.2 The assessment form will be provided by the RIPA Monitoring Officer, should retain the same reference and be kept with the original RIPA paperwork

12.3 The SRO will undertake periodic reviews of the assessment forms and may provide these records as part of any inspection by the Investigatory Powers Commissioner's Office (IPCO).

13 CCTV and Directed Surveillance

13.1 The use of CCTV must be accompanied by clear signage in order for any monitoring to be overt. If it is intended to use CCTV for covert monitoring, for example by using either hidden cameras or without any signs warning that CCTV is in operation, then RIPA authorisation is likely to be required.

13.2 Note 272 of the OSC's 2016 Procedures & Guidance document:

It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

14 Records Management

14.1 Records shall be maintained for a period of at least three years from the cancellation of the authorisation. Following which they shall be securely destroyed in accordance with the council's Retention and Disposal Policy. This can be found on the staffroom at

https://plymouthcc.sharepoint.com/sites/ToolsToDoMyJob/SitePages/Records-Management.aspx

14.2 A copy of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Administrator within five working days of the date of the relevant decision.

14.3 Applicants and Authorising Officers may keep copies of completed RIPA forms, but care must be taken to ensure any copies are stored securely and disposed of in accordance with the council's retention and disposal policy. It is good practice for officers who will be carrying out surveillance to retain a copy of the authorisation as a reminder of exactly what has been authorised. Under the Criminal Procedure and Investigations Act, case files are required to hold original documents for court action

14.4 The following additional information should also be maintained by the Senior Responsible Officer or RIPA Monitoring Officer in relation to any CHIS:

- any risk assessment in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;

14.5 By law, an Authorising Officer must not grant authority for the use of a CHIS unless s/he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. Certain particulars must be included in the records relating to each CHIS, and the records must be kept confidential. Further advice should be sought from the RIPA Monitoring Officer or Senior Responsible Officer on this point if authority is proposed to be granted for the use of a CHIS.

14.6 A Surveillance Log Book should be completed by the investigating officer(s) to record all operational details of authorised covert surveillance or the use of a CHIS. Each service will also maintain a record of the issue and movement of all Surveillance Log Books.

14.7 All RIPA records, whether in original form or copies shall be kept in secure locked storage when not in use.

14.8 Relevant guidance can be found for safeguarding material obtained during surveillance in:
- Chapters 7 and 8 of Covert Human Intelligence Sources Revised Code of Practice
- Chapters 8 and 9 of Covert Surveillance and Property Interference Revised Code of Practice.

15 Error Reporting

15.1 The SRO will undertake a regular review of errors and a written record will be kept by the RIPA monitoring officer of each review.

15.2 Examples of errors are
- Surveillance or property interference activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and the Codes of Practice
- a warrant or authorisation has been obtained as a result of the Council having been provided with information which later proved to be incorrect but on which the Council relied in good faith

15.3 All staff should inform the Authorising Officer of any error who will inform the RIPA Monitoring Officer within 3 working days of any error

15.4 If an error has occurred, the Council must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days. Where the full facts of the error cannot be ascertained within the timescale an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error. This must be followed up with a full report as outlined in paragraph 8.12 of the Covert Surveillance and Property Interference Code of Practice and any Investigatory Powers Commissioner Guidance.

16 Non-RIPA

16.1 Due to the changes brought about by the Protection of Freedoms Act 2012, there may be circumstances whereby it is necessary, and proportionate, to carry out covert surveillance for activities which do not meet the serious crime threshold set out in paragraph 4.5 above. This is referred to in this policy as Non- RIPA

16.2 In such circumstances, staff must complete a non-RIPA form, setting out why such activity is lawful necessary and proportionate and giving due consideration to any potential collateral intrusion.

16.3 Non-RIPA forms must be authorised by an Authorising Officer. However, if the activity relates to an investigation against a member of staff, authorisation must be provided by the Executive Director: Resources and Head of Paid Service. The same considerations and processes as set

out in this policy in relation to RIPA authorisations should be followed save for the need for Magistrates approval.

17 Training

17.1 All officers likely to make applications or authorise them will be required to attend annual training, either by way of a briefing or an e-learning module. It is the responsibility of managers of enforcement teams in particular, to ensure relevant staff are identified and receive such training

17.2 Managers of enforcement teams must ensure that new staff undertake RIPA training within six months of their starting date.

17.3 Authorising Officers must receive regular training on an annual basis. This may be by way of a briefing or an e-learning module.

18 Reporting

18.1 Monitoring of the use of covert activities and surveillance is through a report to Councillors by the Senior Responsible Officer (SRO), which is a required role to oversee compliance with RIPA.

18.2 The SRO is the Director for Corporate Services, who must advise the lead Councillor quarterly and report annually to Council on the use of covert activities and surveillance.

18.3 Reports from the SRO are to include analysis of the covert activities undertaken by service teams and the annual returns required by the RIPA oversight Commissioners; so as to enable Councillors to approve activities as being consistent with this Policy.

19 Review

This Policy will be reviewed annually

APPENDIX A: AUTHORISATION FLOW CHART