Public Document Pack

Ask for Will Stevenson
Email william.stevenson@lichfielddc.gov.uk

District Council House, Frog Lane
Lichfield, Staffordshire WS13 6YU

Customer Services 01543 308000
Direct Line 01543 308199

Wednesday, 21 September 2022

Dear Sir/Madam

AUDIT AND MEMBER STANDARDS COMMITTEE

A meeting of the Audit and Member Standards Committee has been arranged to take place **THURSDAY, 29TH SEPTEMBER, 2022 at 6.00 PM IN THE COUNCIL CHAMBER** District Council House, Lichfield to consider the following business.

Access to the Council Chamber is via the Members' Entrance.

The meeting will be live streamed on the Council's YouTube channel

Yours faithfully

Christie Tims
Chief Operating Officer

To: Members of Audit and Member Standards Committee

Councillors Spruce (Chair), Ho (Vice-Chair), Cross, Grange, Norman, Robertson, Silvester-Hall, White and M Wilcox

AGENDA

1. Apologies for Absence

2. Declarations of Interest

3. Minutes of the Previous Meeting 3 - 6

4. **Leadership Team Response to Questions Raised at the Previous Meeting** 7 - 10

   Letter from Leadership Team. Opportunity for Chief Executive to address any follow up questions.

5. **RIPA reports policy and monitoring** 11 - 34

   Report of the Governance Manager & Monitoring Officer

6. **Verbal Update on the Audit Findings Report for Lichfield District Council 2021/2022**

   Verbal Update from the External Auditors

7. Work Programme 35 - 38

8. **Exclusion of Public and Press**

   RESOLVED: "That as publicity would be prejudicial to the public interest by reason of the confidential nature of the business to be transacted, the public and press be excluded from the meeting for the following items of business, which would involve the likely disclosure of exempt information as defined in Paragraph **3** of Part 1 of Schedule 12A of the Local Government Act 1972"

   IN PRIVATE

9. **Joint Venture**

   Verbal report of the Chief Executive

AUDIT AND MEMBER STANDARDS COMMITTEE

21 JULY 2022

PRESENT:

Councillors Spruce (Chair), Ho (Vice-Chair), Grange, Norman, Robertson, Silvester-Hall, White and M Wilcox

Officers in Attendance: Will Stevenson, Anthony Thomas

Also Present: Kirsty Lees (External Auditor), Councillor Rob Strachan (Cabinet Member for Finance and Commissioning)

1 APOLOGIES FOR ABSENCE

There were apologies from Councillor R. Cross.

2 DECLARATIONS OF INTEREST

There were no declarations of interest during this item. However, Councillor Ho subsequently declared a personal interest during Item 6 (Internal Audit Progress Report) as his family's business is subject to food safety inspections.

3 MINUTES OF THE PREVIOUS MEETING

The minutes of the meeting held on 20 April 2022, previously circulated, were taken as read and approved as a correct record.

4 ANNUAL TREASURY MANAGEMENT REPORT

Anthony Thomas (Assistant Director Finance & Commissioning) presented the annual treasury management report to the committee. Mr Thomas noted that the draft statement of accounts has been completed on 1 July 2022 well in advance of the 31st July deadline and was now in the process of being audited. It was highlighted that the income from capital receipts was higher than the original budget of £296,000 by £219,335. This was primarily due to higher than planned Bromford Right to Buy Sales achieved. The Long Term Pension Liability had seen a roughly £19,000,000 swing from budget to actual, which had naturally had a large impact on the balance sheet. This was mainly due to financial assumptions used in the second of three reports by the Pension Fund Actuary. Other factors were noted including higher working capital and earmarked reserves due to Central Government providing CARF and council tax rebate grants in advance of their spend. The Prudential Indicators will be sent to Full Council later in year, but the committee were assured that all were compliant, and no breaches were recorded.

In response to questions from members regarding the adequacy of reserves, Mr Thomas explained that there had been a book loss in strategic investments (after taking account the volatility reserve) of about £200,000 due to very volatile economic circumstances. It was stated that these conditions may mean that number could swing further in the following months. Noting the loan repayment on 31st March 2022, members asked if it was worth considering an early repayment of the second PWLB loan listed on page 20. Mr Thomas confirmed that this option will be considered. He confirmed officers could also review the potential for increased costs of ongoing projects rolling into other years.

Members noted that SR1 items 'C' and 'D' were still ranked as Red. The committee were informed that the recent dismissal of the relevant Secretary of State had added unwanted uncertainty on this area. When asked if there was a concern about fixed term investments LDC has with unitary authorities, Mr Thomas clarified that the local authorities in question have different support arrangements with their devolved administrations than those in England.

RESOLVED: The committee approved to review the report and issues raised within. The committee also approved to review the actual 2021/22 Prudential Indicators contained within the report.

5 CIPFA RESILIENCE INDEX

Mr Thomas presented the report to committee, explaining that this is the third year the resilience index has been published; it is designed to improve and support local authority financial resilience by showing a range of measures associated with financial risk. The report notes that there are currently more interventions taking place in local government than ever before. The index is backward-looking, so for 2022 it starts to identify the impact of the pandemic. However, looking forward, the strategic risk register continues to show a risk around the availability of finance which is currently in the red zone due to local government finance reform, some residual impact from the Covid-19 pandemic and ongoing inflationary pressures. It was confirmed that the authority is procuring a new insurance provider currently, and officers are interested to see the impact of this change.

Commenting on the figures involved, members agreed that it was wise to err on the side of caution at the present time especially in relation to pay awards.

RESOLVED: The Committee noted the results of the CIPFA Resilience Index for 2022.

6 INTERNAL AUDIT PROGRESS REPORT

The Assistant Director Finance & Commissioning (Anthony Thomas) presented this report in the absence of the Audit Manager (Andrew Wood). Mr Thomas explained that as of this first quarter, 10% of the audit plan has currently been completed. The reasons for this slow pace include several grant assurance items – each requiring a sign off and extra resources required to undertake this assurance work - that were not envisioned initially. The authority is in the process of procuring a general auditor and these resources should be sufficient to compete the audit plan. However, there is a risk that the current rate of organisational change within the council means that target may not be achieved. It was confirmed that the Audit Manager is working towards achieving 90% of the audit plan. All outstanding high priority recommendations will be revisited, and the committee kept updated of their progress.

Members raised significant concerns about the pace of delivery of the audit plan and increasing risk levels. Though sympathetic to the impact of external forces outside the authority's control, the committee noted that it is their obligation to highlight this issue, urging officers to find the resources to tackle these issues before they grow beyond control. They raised five outstanding high priority actions that had been identified for the last five quarters, urging that these be acted upon as soon as possible. Mr Thomas confirmed these issues have been raised with officers and the early stage of the current audit means that there is time for the plan to catch up. However, it was still important to raise the potential risk of external impacts with the committee.

Members requested further detail from Mr Wood regarding the Debtors System discussed on page 48.

RESOLVED: With concerns raised, the committee noted the Internal Audit Quarterly Progress Report, including results for the quarter to 30 June 2022.

7 QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME/PUBLIC SECTOR INTERNAL AUDIT STANDARDS

In the absence of Mr Wood, Mr Thomas presented the report to the committee. As part of the annual self-assessment, Internal Audit operations were reviewed by the Audit Manager and judged to be compliant. These operations would be subsequently subjected to an external quality assessment too. External quality assessments are completed every 5 years, with the last one completed in 2017, and the next one scheduled for this year. At conclusion, this report will be sent to the Audit & Member Standards Committee.

RESOLVED: The committee noted Internal Audit's compliance with the PSIAS and the QAIP.

8 RISK MANAGEMENT UPDATE

In the absence of Mr Wood, Mr Thomas presented the Risk Management report to the committee, including the strategic risk register, last updated by Leadership Team on June 22nd this year. At present, SR1 is the only indicator outside of risk appetite, mainly due to external factors. Horizon Scanning risks identified included voter registration requirements, and the impact of Ukrainian visitors to the district through the potential for breakdown of relationships between hosts and visitors.

Members questioned why SR7 had been reduced from a score of '9' to '6' given that the risk of a cyber-attack has not gone away. Mr Thomas explained that the score was increased significantly at the outbreak of the Russo-Ukrainian War 2022, but at this point there has been no indication of a cyber-attack taking place at LDC. Members noted a recent report from the National Cyber Security Centre specifically suggesting that local authorities should not be complacent about this risk and requested SR7 be reviewed again.

Noting that the AEA recently wrote to the Secretary of State stating that the timescales for voter registration plans were not sufficient, members suggested this risk should be looked at again.

The committee raised significant concerns that 5 out of 7 risks are currently scored '9' and raised the possibility of a ceiling on the cumulative total of risk scores that could be deemed acceptable. Members expressed keen interest in inviting the Chief Executive and managers responsible for areas of risk to come before the next committee in September 2022 to provide further detail and accountability.

Members requested clarification on why SR2 has not increased through a period of significant managerial change within the council.

RESOLVED: The committee noted the risk management update and received assurance on actions taking place to manage the Council's most significant risks, subject to the significant concerns raised by the committee. Members requested that the Chief Executive and a manager responsible for an area of risk, both be invited to the next meeting.

9 WORK PROGRAMME

RESOLVED: Members noted the contents of the work programme for the 2022/23 year.

(The Meeting closed at 7.06 pm)

CHAIR

Draft Response to Audit and Member Standards Committee Questions and Comments 21 July 2022

Treasury Management Report

- Councillor Ho wanted assurance that the waste from the office refurbishment was disposed of in a sustainable way.
    - Harrow Green were selected to ensure that nothing from the site went to landfill. Their website provides full details about corporate responsibility however a summary is provided in the paragraphs below:
        - Corporate Social Responsibility is woven into the way we conduct business because we believe in sustainability and in operating in a world that will be better tomorrow than it is today.
        - Our trading practices are structured in a way that is sustainable, particularly in regards to recycling and asset disposal, which is a big part of the way we do business. We apply a 0% to landfill policy with all the assets we dispose for our customers and take other measures to ensure our approach is as green as we can make it.
        - Through our Re-Fresh programme, we dispose of our customers' no-longer-needed furniture and IT equipment in the most environmentally friendly way possible by recycling, refurbishment and re-sale or charitable donation, which guarantees the best possible outcome for both our customers and the environment.
        - We also take strides to support the communities in which we operate by offering our services free of charge whenever they're required by local charities.
    - In addition, chairs were provided to schools and other local organisations and social media was used to further promote availability for use by the wider community.
- Councillor Robertson asked if additional capacity should be considered to expedite delayed capital spend such as the Coach Park.

  The capacity related specifically to capital project delivery capacity has been increased in relation to:
    - A major projects team was created a number of years ago.
    - In terms of Lichfield City Masterplan projects, further capacity was procured through an Interim Director of Regeneration and following their departure, two further programme managers will be recruited.
    - A programme director was procured together with further additional capacity specifically to deliver the Being a Better Council programme.
    - We have appointed Lambert Smith Hampton (LSH) to provide additional capacity as a managed partner principally to deliver the Lichfield City Masterplan programme however they are able to provide additional capacity in other areas of the Council.
    - Council has also recently approved a budget of £1.2m that can be used to support any other capacity investment such as digital support and further apprenticeships that will enable the delivery of Council priorities.
- Councillor Robertson asked what the balance on the Burntwood Sinking Fund currently is

  The current balance is £69,000 and any investment needs in excess of this budget will need to be funded from the property planned maintenance budget, reprioritisation of existing budgets or through the use of reserves.

Internal Audit Progress Report

- Internal Audit Plan delivery progress and the lack of progress in addressing the 5 high priority recommendations and the lack of change in the period for the medium priority recommendations.

  We have made two attempts using different recruitment approaches to recruit a Senior Auditor without success due to a very challenging recruitment market for auditors. We have now identified an external audit firm that is able to provide additional capacity to support delivery of the approved internal audit plan.

  Leadership Team have taken on board the Committee's views regarding the lack of progress on implementing audit recommendations and confirm that target dates have been set and progress will be reviewed on a monthly basis as part of the risk management review.

  We can confirm therefore we will provide updates to the Committee on the outcome of the 5 high priority recommendation reviews as they occur.

- In terms of the debtor's suspense account issue identified and assurance this was being addressed by Management.

  To confirm payments have been allocated as follows:

  - M0007443646 £0.47 has been allocated to invoice M0075905147. This was raised as invoice M0007443646 was at a nil balance when we migrated over to Civica Debtors and we've since received some dividend payments.
  - P0000061109 £1,057.88 has been allocated to M0075895671. The payment was from New Look for Rent, which is now based on monthly turnover and we were awaiting confirmation of the figures before the invoice was raised.
  - The following 3 payments were moved out of the suspense account in order for it to be cleared for the financial year end and were allocated to an invoice with the debtor name Unidentified Payments. We are still in the process of trying to contact the customers as these payments are to be refunded.

    P0000050044 £20.00

    M0007543375 £25.00

    M0007563744 £116.88
  - As at 1st August 2022 we have two items in the suspense account M0007274972 £30.00 and M0007188376 £82.71, these are currently being reviewed/investigated.

  Discussions and communications held with the Income Recovery Officer has outlined that the number of items entering suspense are relatively small in number i.e., 1 every couple of weeks. However, the Income recovery Officer did outline that on a daily basis the cash receipting reports are reviewed and these will list any items allocated to suspense account. The duty officer for the recovery team should then try and deal with these issues as they arise.

  The section does not have a specific target, however this is due to the low number of items entering suspense and that these are resolved as soon as practicable once they are identified.

Risk Management Update

- The Committee acknowledged only one red risk however there was a concern at the number of risks in the amber area and the number of factors indicating an increase in the risk environment at the Council.

  It is acknowledged that the strategic risk register does show six (86%) strategic risks that are in the amber area of the risk matrix and this could potentially impact on the Council's ability to deliver its strategic plan. However, there are several key points to make:

  - Strategic Risk registers are focussed on each local authority's objectives and risks however we do regularly review other District Council Corporate/Strategic Risk Registers to ensure we take an external perspective.
  - A number of the risks in the Council's Strategic Risk Register are generic across local government and are also influenced by external factors such as the economic/statutory environment as evidenced by the latest analysis of other District Council risk registers that is shown below:

Local Authority	Lichfield	Cannock Chase	Tamworth	Wychavon	Staffordshire Moorlands	Worcester City	South Staffordshire
Strategic / Corporate Risks	**7**	**6**	**6**	**19**	**16**	**26**	**8**
Red / High	1	4	0	0	8	3	1
%	14%	67%	0%	0%	50%	12%	13%
Finance	X	X			X	X	
Development Plan						X	
Resilience / Capacity of teams		X					
Employee Wellbeing					X		
Governance/Statutory							
ICT/Cyber Attack					X	X	
Local Economy		X					
Key Suppliers		X					X
World Events					X		
External Funding					X		
Contract Management					X		
Asset Investment					X		
Safeguarding					X		
Amber / Medium	6	2	5	9	7	5	6
%	86%	33%	83%	47%	44%	19%	75%
Green / Low	0	0	1	10	1	18	1
%	0%	0%	17%	53%	6%	69%	13%

  - The Council takes an active approach to Risk Management through Leadership Team and Audit and Member Standards Committee regularly reviewing the Strategic Risk Register, Service Risk Registers and Horizon Scanning.
  - The Internal Audit Team undertake planned reviews of the Risk Management approach with the last taking place in Jan/March 2022 with a Reasonable assurance level that will be reported, verbally, to the Audit and Member Standards Committee on 21st September 2022.
  - The expanded Value for Money Assessment undertaken by the External Auditors is focussed on three areas – financial resilience, governance and economy, efficiency and effectiveness. All three of these areas will consider the Council's approach to risk management and the Annual Audit Report reported to Audit and Member Standards Committee on 20 April 2022 indicated no risks or significant weaknesses identified.
  - The Chief Executive will attend the next meeting to provide assurance that these issues are being prioritised and managed.

This page is intentionally left blank

REGULATION OF INVESTIGATORY POWERS ACT 2000

Report of the Monitoring Officer

Date:	21 September 2022
Agenda Item:	
Contact Officer:	Mark Hooper
Tel Number:	308064
Email:	Mark.hooper@lichfielddc.gov.uk
Key Decision?	**NO**
Local Ward Members	Full Council

AUDIT & MEMBER STANDARDS COMMITTEE

1. Executive Summary

1.1 The Council has adopted a policy and procedures for carrying out surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.2 The policy, and the use of directed surveillance /covert human intelligence sources, is reviewed and reported to the Audit and Standards Committee on an annual basis.

2. Recommendations

2.1 That the Audit & Member Standards Committee notes the RIPA monitoring report for the 2021-2022 financial year.

2.2 That the Audit & Member Standards Committee approves the updates to the Corporate Policy and Procedure for RIPA as set out in **Appendix 1**.

2.3 3. Background

3.1 The Regulation of Investigatory Powers Act (RIPA) was introduced in 2000 to give public authorities a legal framework to follow if they are carrying out surveillance.

3.2 The RIPA Code of Practice produced by the Home Office in April 2010 and updated in January 2016 introduced the requirement to produce reports to elected members to demonstrate that the Council is using its RIPA powers appropriately and complying with its own Code of Practice when carrying out covert surveillance.

3.3 This requirement relates to the use of *directed surveillance* and *covert human intelligence sources* (CHIS).

3.4 **Directed Surveillance** is defined as surveillance which is covert and pre-planned, but not intrusive and undertaken:

- For the purpose of a specific investigation or operation
- In such a manner as is likely to result in obtaining private information about a person.

3.5 It does not include surveillance which is an immediate response to events or circumstances where it is not reasonably practicable to obtain an authorisation.

3.6 **A CHIS** is a person who establishes or maintains a relationship with a person in order to covertly obtain or disclose information.

Use of directed Surveillance and CHIS

3.7 The Council has not used directed surveillance during the review period.

3.8 There have also been no authorisations for the use of CHIS.

Training

3.9 The RIPA Co-ordinator and all Authorising Officers completed training on 3 February 2021.

Annual Review of Policy

3.10 The Investigatory Powers Commissioner's Office completed an inspection in February 2021 and noted the failure to undertake an annual review of the RIPA policy and procedures in 2020 due to Covid pressures.

3.11 An annual report on the use of RIPA has been provided to members each year, but the policy and procedures have not been reported since their introduction in 2018. This will now form part of the annual report going forward.

3.6 The policy at Appendix 1 addresses the use of social media, and what constitutes surveillance requiring authorisation. This is of particular relevance given the widespread use of social media and will form an important component of officer training.

Alternative Options	Obligations arising under RIPA for the authority are statutory therefore the only option is compliance.
Consultation	Input into the updated policy has been sought from SSLegals, staff using any form of overt or covers surveillance and investigation techniques. The updated policy reflects comments and observations from IPCO
Financial Implications	Support for the RIPA obligations and functions are met from existing budget and existing staff resources.
Approved by Section 151 Officer	
Legal Implications	This report covers our statutory duty to keep our RIPA policy under review on an annual basis and ensuring any authorisations sought will be done so in compliance with the law.
Approved by Monitoring Officer	Yes
Contribution to the Delivery of the Strategic Plan	A good council.

Equality, Diversity and Human Rights Implications	The recording of applications, authorisations, renewals and cancellations of investigations using covert surveillance techniques or involving the acquisition of communications data is covered by the Regulation of Investigatory Powers Act 2000. The Regulation of Investigatory Powers Act was introduced to regulate existing surveillance and investigation in order to meet the requirements of Article 8 of the Human Rights Act. Article 8 states: Everyone had the right for his private and family life. His home and his correspondence, there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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. RIPA investigations can only be authorised by a local authority where it is investigating criminal offences which (1) attract a maximum custodial sentence of six months or more or (2) relate to the sale of alcohol or tobacco products to children. There are no risk management or Health and Safety implications.

Environmental Impact	None arising from this report.

Crime & Safety Issues	The recommendation(s) will impact (positively) on our duty to prevent crime and disorder within the District (Section 17 of the Crime and Disorder Act, 1988). The legislation requires the Authority to record and monitor all RIPA applications, keep the records up to date and report yearly to a relevant Committee.

GDPR/ Privacy Impact Assessment	RIPA investigations will capture personal data and fall within the scope of the considerations of the authority. The use of a Human Rights Assessment will consider privacy impacts on a case by case basis.

	Risk Description & Risk Owner	Original Score (RYG)	How We Manage It	Current Score (RYG)
A	Failure to obtain RIPA authorisation or comply with RIPA	LIKELIHOOD IMPACT SEVERITY	Regular Training/Keeping Records of authorisation/Notifying staff of changes to procedure/policy	LIKELIHOOD IMPACT SEVERITY
B	Staff using covert practices unwittingly	LIKELIHOOD IMPACT SEVERITY	Regular training and awareness sessions/reminders	LIKELIHOOD IMPACT SEVERITY

Background documents	
Relevant web links	

This page is intentionally left blank

CORPORATE POLICY & PROCEDURES

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

NOTE: The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application this Corporate Procedures Document refers to 'Authorising Officers'. For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to 'Designated Officers' under RIPA.

Acknowledgements*:*

The Council wishes to acknowledge the work of Birmingham City Council, Stratford Upon Avon District Council and Southwark Council in this area. This procedure is based upon their precedent policies with updated advice from South Staffordshire Legal Service (SSLegals).

Version Date: June 2022

CONTENTS PAGE

A. INTRODUCTION AND KEY MESSAGES

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA') and the Home Office Codes of Practice on Covert Surveillance and Acquisition of Communications Data. The Home Office Codes of Practice can be found at: https://www.gov.uk/government/organisations/home-office/series/ripa-codes

2. Where reference is made in this document to the Senior Responsible Officer (SRO) this means the Monitoring Officer, whose duties are to:-

   (a) ensure the integrity of the Council's RIPA processes
   (b) ensure compliance with RIPA legislation and codes of practice
   (c) engage with the OSC inspector during an inspection
   (d) implement post-inspection recommendations
   (e) exercise oversight of all authorisations
   (f) ensure Authorising Officers are trained to an appropriate standard
   (g) issue regular reminders and updates on RIPA to all staff (see appendix 2)
   (h) review and report on the operation of the RIPA policy annually to the Audit and Standards Committee

3. Councillors have a role to play in reviewing the Council's use of RIPA to ensure that it is being used consistently with this procedure document. They will also ensure that the policy is fit for purpose. However, councillors will not be involved in making decisions on individual authorisations.

4. Where reference is made in this document to the RIPA Co-ordinating Officer this means the Monitoring Officer or a Governance Officer designated by the Monitoring Officer to perform that role, the duties being to:-

   (a) maintain the Central Register of authorisations
   (b) collate original applications, reviews, renewals and cancellations
   (c) oversee submitted RIPA documents
   (d) raise RIPA awareness in the Council
   (e) advise applicants and issue a unique reference number
   (f) devise and implement a training programme (see Appendix 2)
   (g) liaise with SSlegals to ensure effective updates to the code

5. The authoritative position on RIPA is, of course, the Act itself and any officer who is unsure about any aspect of RIPA should, if unsure, **If any doubt arises, the Home Office Code of Practice should be consulted; the Code of Practice takes precedence over this guidance.**

   - **Covert Human Intelligence Sources**
   - **Covert Surveillance**
   - **Communications Data .**

6. Appropriate training and development (including refresher training) will be provided or arranged by the RIPA Co-ordinating Officer for Authorising Officers and Investigating Officers.

7. The RIPA Co-ordinating Officer will maintain and check the Central Register of all RIPA Authorisations, Reviews, Renewals, Cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to ensure the RIPA Co-ordinating Officer receives the originals of the relevant Forms within 1 week of authorisation, review, renewal, cancellation or rejection.

8. RIPA and this Policy are important for the effective and efficient operation of the Councils' actions with regard to covert investigations. This Policy will, therefore, be kept under annual review by the SRO. **Authorising Officers must bring any suggestions for continuous improvement of this Policy to the attention of the SRO at the earliest possible opportunity**. If any of the Home Office Codes of Practice change, this Policy will be amended in light of these changes.

In terms of internal monitoring of e-mails and internet usage, it is important to recognise the important interplay and overlaps with the relevant Council's e-mail and internet policies, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018. RIPA forms should only be used wherever relevant and are only -3- relevant where the criteria listed on the forms are fully met. Under normal circumstances, the Council's e-mail and internet policies should be used, as any surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA.

9. This update includes the changes to RIPA brought about by the Protection of Freedoms Act 2012. This includes judicial approval of all covert surveillance carried out by local authorities and restricting use of directed surveillance to serious criminal offences.

10. **At no time should the Council undertake any surveillance that interferes with any private property. Placing tracking devices on a subject's vehicle or person is not authorised for local authorities and must not be used.**

11. **The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in investigation matters.**

B. AUTHORISING OFFICER RESPONSIBILITIES

1. It is essential that Authorising Officers take personal responsibility for the effective and efficient operation of this Policy. Authorising Officers are listed in Appendix 1. They can be added to or substituted by the SRO using normal delegation procedures as necessary.

2. The SRO has and will ensure that a sufficient number of Authorising Officers are, after suitable training on RIPA and this Policy, duly authorised to take action under this Policy with further guidance and support available from SSLegals.

3. **It will be the responsibility of the RIPA Co-Ordinating Officer to ensure that investigating officers are suitably trained as 'Applicants' so as to avoid common mistakes appearing on RIPA Forms.**

   Authorising Officers must ensure that staff who report to them follow this Policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations and gain expert advice when using surveillance or any new investigation procedures before any action is *taken* in compliance with this Policy.

4. Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances should an Authorising Officer approve any RIPA form unless, and until they are satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, they should obtain prior guidance on the same from the Council's Health & Safety Manager and the SRO.

5. Authorising Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and ensure that the original forms are sent to the RIPA Co-ordinating Officer in a **sealed** envelope marked '**Strictly Private & Confidential' or scanned in via email and the hard copy kept secure**. Forms must be provided to the RIPA co-ordinating Officer within 5 working days of signing by the Authorising Officer. Any failure to comply exposes the Council to unnecessary legal risks and criticism from the Office of Surveillance Commissioners. Any cancellations must be dealt with promptly.

6. The likelihood of obtaining **confidential information** during surveillance must be given prior thought before any authorisation forms are signed, as failure to do so may invalidate the admissibility of any evidence obtained. Furthermore, thought must be given before any forms are signed to the retention and disposal of any material obtained under a RIPA Authorisation.

7. Confidential personal information (information where a high degree of privacy may be expected due to the relationship between the parties concerned e.g. solicitor/client; priest/parishioner; journalist/informant; counsellor/consultee etc.) will not be acquired as a result of any covert surveillance, the use of CHIS and the acquisition and disclosure of communications employed by the Council. Where there is any identified risk of acquiring confidential information prior to authorisation, then such activity shall only be authorised by the Chief Executive or Chief Operating Officer.

The Authorising Officer must ensure proper regard is had to **necessity and proportionality** of the surveillance before any forms are signed. 'Stock phrases' or cut and paste narrative must be avoided at all times as the use of the same may suggest that insufficient detail had been given to the particular circumstances of any person likely to be the subject of the surveillance. Any **equipment** to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

C. GENERAL INFORMATION ON RIPA

1. The Council takes its statutory responsibilities seriously and will, at all times, act in accordance with the law and take necessary and proportionate action in this regard. The Head of Governance & Performance is duly authorised by the Council to keep this document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administration and operational effectiveness, the SRO is also authorised to add or substitute officers authorised for the purpose of RIPA in consultation with the Chief Executive or Chief Operating Officer.
2. The Council has adopted a policy to the effect:
   - that all covert surveillance operations, the use of CHIS and the acquisition and disclosure of communications data conducted by the Council should comply with the requirements of RIPA and the Home Office Codes of Practice;
   - that only the officers detailed in Appendix 1 shall be permitted to authorise a covert surveillance exercise, a CHIS or the acquisition of communications data, subject in each case to the restrictions noted in that appendix.
   - that, where it is judged necessary to obtain it, the acquisition of communications data shall be undertaken through a Clearing House, thus avoiding the need for the Council to employ a Single Point of Contact (SPOC) under RIPA (and associated legislation) and the Home Office Code of Practice;
   - that covert surveillance; CHIS and the acquisition and disclosure of communications data shall only be employed when necessary for the purposes of the prevention or detection of crime or preventing disorder and when such action is considered to be proportionate to the offence or disorder concerned; and
   - that this document and the Home Office Codes of Practice be brought to the attention of all the staff who may carry out covert surveillance or the use of CHIS.

3. Operations under RIPA can be authorised only on the following ground:- **For the purpose of preventing or detecting crime or of preventing disorder**

4. In order for a directed surveillance authorisation to be made, the serious crime test must be passed. This means there must be a criminal offence and the offence under investigation must carry a sentence of 6 months imprisonment. There is an exception for underage sale operations in respect of alcohol and tobacco sales.
5. In assessing whether or not the proposed surveillance is necessary and proportionate, the authorising officer must consider other appropriate means of gathering the information. The least intrusive method will be considered proportionate by the Courts. Surveillance activity should only be used as a last resort.

6. RIPA provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS')** – e.g. undercover agents. However, this Council is reluctant to use CHIS as an investigatory tool, and if any such application is contemplated prior advice must be sought from the RIPA Co-ordinating Officer. RIPA also permits local authorities to compel telecommunications and postal companies to obtain and release communications data to themselves, in certain circumstances. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention

is **necessary** and **proportionate**. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

7. Directly employed Council staff and external agencies working for the Council are covered by RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's Authorising Officers with relevant advices from SSLegals.

8. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Local Government Ombudsman, and/or the relevant Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with covert investigations comply with this Policy and any further guidance that may be issued, from time to time, by the SRO.

9. The Council treats the powers given to it under RIPA very seriously and expects Authorising Officers and Investigating Officers to do so. Failure to adhere to this Policy by Authorising Officers or Investigating Officers may result in disciplinary action being taken against them by the Council.

10. **Human Rights Act Assessments**

The Council may wish to undertake surveillance (e.g. noise monitoring prior to service of an Abatement Notice) and may on occasion determine that this should be on a covert basis. Noise monitoring is usually notified to the person being monitored and therefore is outside of RIPA. However, if in particular circumstances, covert surveillance is considered appropriate outside of RIPA, then a full Human Rights Act (HRA) assessment should be undertaken. The same forms as for RIPA should be used, as HRA Assessment Forms, and be authorised internally in the usual way (there is no need for Judicial Approval). This will assist in considering and assessing the issues and also protecting the Council if challenged under Human Rights Act.

11. **Social Networking Sites and Internet Sites**

Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required for incidental viewing (See HRA above). However, persistent access is not permitted unless prior authorisation is obtained from an Authorising Officer.

If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a social networking site, asks to join a site / group, or monitors the site on an ongoing basis. Any interaction on social media will require use of authorisation. Officers must not use their own social media accounts for this purpose.

Should such "covert profiles" be used to undertake surveillance the RIPA Co-ordinating Officer should be provided with details of who has used these profiles and when; and a record of what information was recorded should be made available to the relevant Authorising Officer for review.

12. A flowchart of the procedure for Magistrates' approval of surveillance operations is at **Appendix 3**.

D. TYPES OF SURVEILLANCE

1. **'Surveillance'** 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.

2. **Overt Surveillance**

   Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. parking wardens walking through town centres).

3. Similarly, surveillance will be overt if the subject has been told it will happen e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded 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 identifying themselves to the owner/proprietor to check that the conditions are being met.

4. **Covert Surveillance**

   Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place (Section 26(9) (a) of RIPA). It cannot, however, be "necessary" if there is reasonably available an overt means of finding out the information desired.

5. RIPA regulates three types of covert surveillance: Directed Surveillance, Intrusive Surveillance and the use of Covert Human Intelligence Sources (CHIS).

6. **Directed Surveillance** is surveillance which:-

   - is covert;
   - is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance or any interference with private property);
   - is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it;
   - is pre-planned; and
   - is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual whether or not that person is specifically targeted for purposes of an investigation (Section 26(10) of RIPA).

7. **Private information** in relation to a person includes any information relating to their private and family life, their home, their correspondence and their business relationships. 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. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about them and others that they come into contact, or associate, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera(s) are to be directed for a specific purpose to observe particular individual(s), authorisation will be required. The way a person runs their business may also reveal information about their private life and the private lives of others.

9. **For the avoidance of doubt, Authorising Officers for the purpose of RIPA can authorise 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this Policy are followed. Authorisation can only be granted if it is necessary for the purposes of investigating serious crimes (as defined in Section G – paragraph 9) and relevant advice has been sought.**

10. **Intrusive Surveillance**

This is when the 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.

Surveillance of a place ordinarily used for legal consultation; at a time when they are being used for such consultations is also a form of intrusive surveillance.

11. Areas of a building that are readily visible and accessible to the public are not residential premises. For example, a communal stairway, canteen, reception area, driveway, front garden and so on.

12. **Intrusive Surveillance cannot be carried out or approved by the Council. Only the police and other law enforcement agencies are permitted to use such powers. Likewise, the Council has no statutory powers to interfere with private property.**

13. **"Proportionality"**

Proportionality involves balancing the intrusiveness of the activity on the target subject and others who might be affected by it against the need for the activity in operational terms. Consider the expected benefit to the investigation of the surveillance. The activity will not be proportionate if it is excessive in the circumstances – each case will be judged and be unique on its merits – or if the information which is sought could be reasonably be obtained by other less intrusive means. All such activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Extra care should also be taken over any publication of the product of the surveillance.

When authorising covert surveillance, the following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result including overt methods of evidence gathering;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

14. **Examples of different types of Surveillance**

Type of Surveillance	Examples

Overt	Police Officer or Parks Warden on patrol Signposted Town Centre CCTV cameras (in normal use). Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	CCTV cameras providing general traffic, crime or public safety information. Viewing of publicly available social media profile and postings. *(Use of HRA)*
Directed must be RIPA authorised	Covert CCTV cameras at a fly-tipping hotspot. Covert and targeted following of a benefit claimant who is suspected of failing to declare earnings from a job, can be by investigators/observation, CCTV or social media.
Intrusive or interfering with private property –**the Council cannot do this!**	Planting a listening or other electronic device (bug) or camera in a person's home or in / on their private vehicle or on their person. Surveillance of a place used for legal consultations.

15. **Further Information** on different types of surveillance can be found in the Home Office Code of Practice on Covert Surveillance:
https://www.gov.uk/government/organisations/home-office/series/ripa-codes

16. **Confidential Information**

Special safeguards apply with regard to confidential information relating to legal privilege, personal information, journalistic material and confidential constituent information. Only the Chief Executive, or in his/her absence an appointed deputy, can authorise surveillance likely to involve confidential information. The Investigating Officer must understand that such information is confidential and cannot be obtained. Further guidance is available in the Home Office Codes of Practice:
https://www.gov.uk/government/organisations/home-office/series/ripa-codes

17. **Collateral Intrusion**

Before authorising surveillance, the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (known as collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

18. Those carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. If the original authorisation is sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required. Further guidance is available in the Home Office Code of Practice.

19. **Retention and destruction of product of surveillance**

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by the Council relating to the handling and storage of material.

E. COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

1. Who is a CHIS?

This is someone who establishes or maintains a personal or other relationship for the covert purpose of using that relationship to obtain information. This would include, for example, a situation where a Council officer establishes a relationship with another person through social media, even where there is no physical contact with the CHIS. However, a CHIS does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information (e.g. benefit cheat hotlines).

THE COUNCIL IS RELUCTANT TO USE CHIS, AND IF AN OFFICER IS CONTEMPLATING THE USE OF THIS TYPE OF SURVEILLANCE HE/SHE MUST OBTAIN PRIOR ADVICE FROM THE SRO OR RIPA CO-ORDINATING OFFICER. HOWEVER, THE COUNCIL DOES RECOGNISE THAT CIRCUMSTANCES MAY ARISE THAT MAKE THE USE OF A CHIS NECESSARY AS AN INVESTIGATIVE TOOL.

In order to mitigate the risk of a CHIS arising inadvertently during the course of an investigation the Council will ensure that Authorising and Investigating Officers are trained in the identification of a CHIS as part of corporate training on RIPA.

Management of a CHIS

Always seek advice from the SRO or the RIPA Co-ordinating Officer prior to authorising a CHIS. In all cases, prior to authorising a CHIS a risk assessment must be undertaken in relation to the source. A CHIS may only be authorised if there will at all times be an officer (referred to as the handler) within the Council who will have day to day responsibility for dealing with the source on behalf of the Council, in order to protect both the security of the source. The handler is normally the Investigating Officer. In addition, another officer must be appointed (known as the controller) who will have general oversight of the use made of the source. This person is normally the Investigating Officer's line manager. Lastly, an officer must be identified to maintain certain prescribed records (as specified in the codes of practice) of the use made of the source.

Special requirements apply to the use of a vulnerable individual or a juvenile as a CHIS. Before considering the authorisation of such a person the Authorising Officer must seek legal advice from the RIPA Co-ordinator or the SRO.

2. Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product would require authorisation as a CHIS.

3. **Anti-social behaviour activities (e.g. noise, violence, race etc.)**

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior authorisation.

If the sound recording equipment is so sensitive that it can record conversations as if you were in the room, this would be intrusive surveillance and cannot be authorised under RIPA. The noisemaker shall be warned so that it can be overt surveillance.

F. ACQUISITION OF COMMUNICATIONS DATA

What is Communications Data?

1. Communication data means any traffic or any information that is or has been sent over a telecommunications system or postal system, together with information about the use of the system made by any person.

2. RIPA defines communications data in three broad categories: -

(a) **Section 21(4) (c) Information about communications service users.**
This category mainly includes personal records supplied to the Communications Service Provider (CSP) by the customer/subscriber. For example, their name and address, payment method, contact number etc.

(b) **Section 21(4) (b) Information about the use of communications services.**

This category mainly includes everyday data collected related to the customer's use of their communications system. For example, details of the dates and times they have made calls and which telephone numbers they have called.

(c) **Section 21(4) (a) Information about communications data (traffic data).**

This category mainly includes network data generated by the CSP relating to a customer's use of their communications system that the customer may not be aware of. For example, cell site data and routing information.

3. **The Council only has power to request data under Section 21(4) (b) and Section 21(4) (c) but NOT Section 21(4) (a).**

What types of communications data is available to the Council?

4. **Section 21(4)(c) - Information about communications service users**

- Name of account holder/subscriber;
- Installation and billing address;
- Method of payment/billing arrangements;
- Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered – not where it is collected from or delivered to);
- Other customer information such as any account notes, demographic information or sign up data (not passwords or personalised access information).

5. **Section 21(4)(b) - Information about the use of communications services**

- Outgoing calls on a landline telephone or contract or prepay mobile phone
- Timing and duration of service usage;
- Itemised connection records;
- E-mail logs (sent);
- Information about the connection, disconnection and re-connection of services;
- Information about the provision of conference calling, call messaging, call waiting and call barring;
- Information about the provision and use of forwarding/redirection services (postal and telecom);
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

What Purpose Can Communications Data Be Accessed?

6. The Councils can only access communications data for the **prevention and detection of crime or preventing disorder** (Section 22(2) (b) of RIPA).

Applying for Communications Data

7. The Investigating Officer must complete an application form: - https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2 in full with no sections omitted. (The form is subject to inspection by the Interception of Communications Commissioner and the applicant may be asked to justify their application).

8. Two forms of authorisation are possible: -

(a) An authorisation under Section 22(3) of RIPA. This authorises the applicant to personally extract the data from the CSP's records. (This will rarely be used by the Council as its intended use is where there may be a security breach at the CSP and asking the CSP to provide the data would forewarn or alert the subject).

(b) A notice under Section 22(4) of RIPA requiring the CSP to extract the communications data specified from its records and to send that data to the Single Point Of Contact (SPOC) (normal request).

The applicant must indicate which authorisation they seek.

9. The application form is then submitted to the SPOC for the Council, which is the National Anti-Fraud Network (NAFN).

10. The idea of only having one point of contact for each public authority was agreed between the Home Office and the CSP's to ensure data was only supplied to those entitled to obtain the data. Only the SPOC can acquire communications data on behalf of the Council.

11. The SPOC will then assess whether the form is completed properly, that the request is lawful, the request is one to which the CSP can practically respond and that the cost and resource implications for the CSP / Council are within reason.

12. The SPOC will then submit the form to the Authorising Officer for authorisation. (As previously stated, the application form is subject to inspection by the Interception of Communications Commissioner and therefore the Authorising Officer may be called upon to justify any decisions made).

13. The application must then be approved by a Magistrate. The Investigating Officer should liaise with the RIPA Co-ordinating Officer to obtain this authorisation.

14. The RIPA Co-ordinating Officer or their authorised officer will arrange a hearing with the Court to seek the Magistrate's approval. They should provide the Court with the application form and supporting information. The Investigating Officer will be required to attend Court with the Council's solicitor to seek the Magistrate's approval.

15. Guidance on the procedure for seeking Magistrate's approval can be found at https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

16. If the application is rejected by either the SPOC or the Magistrates, the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection.

17. Once authorised by the Magistrates, the SPOC will forward the application to the CSP.

18. Once the data sought is returned to the SPOC, a copy of the information will be passed to the applicant.

19. All original documents will be retained by the Governance Team.

20. There are a number of other administrative forms that the SPOC's are obliged to complete as the application is progressed, although these will not necessarily involve the Investigating Officer.

21. Authorisations to collect communications data under s22 (3) have a life span of one month. However, they can be renewed by serving a new authorisation or notice for further months, within any time within the current life of the notice. Magistrates would need to approve any renewal.

22. If you are at all unsure about anything to do with acquiring communications data, please contact the SPOC, the SRO or the RIPA Co-ordinating Officer for advice **before** applying.

G. AUTHORISATION PROCEDURES

1. Directed surveillance can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

2. All RIPA surveillance authorisations (i.e. Directed Surveillance and the acquisition of Communications Data) must be approved by a Magistrate before they take effect.

Authorising Officers

3. RIPA Forms can only be signed by Authorising Officers.

4. Authorisations under RIPA are separate from delegated authority to act under the relevant Council's Scheme of Delegation. All RIPA authorisations are for specific investigations only, and must be reviewed, renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time! The Authorising Officer must ensure that an authorisation is cancelled as soon as it is no longer required.**

Training Records

5. Appropriate training will be given (or approved) by the RIPA Co-ordinating Officer before Authorising Officers are certified to sign any RIPA Forms.

6. If the SRO feels that an Authorising Officer has not complied fully with the requirements of this Policy, or the training provided to them, he/she is duly authorised to retract that officer's authorisation until they have undertaken further approved training.

Application Forms

7. Only the Home Office approved RIPA forms must be used. Any other forms used, will be rejected by the Authorising Officer and/or the RIPA Co-ordinating Officer. All the RIPA forms can be found at: https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2

Grounds for Authorisation

8. Acquisition of communications data can only be authorised by the Council on the grounds of preventing/detecting crime/disorder. No other grounds are available to local authorities.

9. Directed Surveillance can only be authorised for investigating serious criminal offences. 'Serious' means criminal offences that are punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment. Serious criminal offences would include dangerous waste dumping and serious or serial benefit fraud. We cannot carry out Directed Surveillance for offences that would only result in a fine or less than sixth month's imprisonment, such as littering or dog fouling.

Assessing the Application Form

10. Before an Authorising Officer signs an application form, they must:-

(a) Be mindful of this Policy, the training provided or facilitated by the RIPA Co-ordinating Officer and any other guidance issued, from time to time, by the SRO, SSlegals or the Home Office on such matters.

(b) Satisfy themselves that the RIPA authorisation is:-

(i) **in accordance with the law**;

(ii) **necessary** in the circumstances of the particular case and on the grounds of preventing or detecting crime or preventing disorder;

(iii) for directed surveillance, it must be necessary for the investigation of a serious criminal offence; **and**

(iv) **proportionate** to what it seeks to achieve (see comments in Section D).

(c) **In considering necessity, remember that the surveillance must be necessary for the purpose of preventing or detecting crime or of preventing disorder. There should be details of the crime(s) relied upon in the application form. In addition you need to ensure that the crime attracts a custodial sentence of a maximum of 6 months or more, or involves an offence under section 146, 147 or 147A of the Licensing Act 2003. Authorising Officers also need to demonstrate that there were no other means of obtaining the same information in a less intrusive way.**

(d) In assessing whether or not the proposed surveillance is proportionate, an Authorising Officer should consider the following:-

(i) balance the size and scope of the proposed surveillance against the gravity and extent of the perceived crime or offence;

(ii) will the surveillance method to be used cause the least possible intrusion on the target and others?

(iii) is the surveillance an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the evidence? and

(iv) what other methods of evidence gathering have been considered and why were they not used?

(e) Always remember that the **least intrusive method will be considered proportionate by the courts.**

(f) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality. The duration of the surveillance will not be a consideration in determining proportionality.

(g) Set a date for review of the authorisation and review on that date using the relevant form. Authorisations for directed surveillance should be reviewed at least once a month.

(h) Ensure that the originals of all RIPA forms (applications, review, renewal and cancellation) are forwarded to the RIPA Co-ordinating Officer, **within 5 working days of the relevant authorisation, review, renewal, cancellation or rejection**.

(i) In the case of notices relating to communications data, these will be kept by the RIPA Co-ordinating Officer.

(j) **If unsure on any matter, obtain advice from the SRO or the RIPA Co-ordinating Officer before signing any forms**.

Magistrate's Approval

11. After the Authorising Officer has signed the RIPA application form, it must be approved by a Magistrate before the operation can commence. The Investigating Officer should liaise with the RIPA Co-ordinating Officer to seek this authorisation.

12. The RIPA Co-ordinating Officer will arrange a hearing with the court to seek the Magistrate's approval. They should provide the court with the RIPA application form (signed by the Authorising Officer) and supporting information. The Investigating Officer and Authorising Officer will be required to attend court with an appointed Solicitor to seek the Magistrate's approval.

13. Guidance on the procedure for seeking Magistrate's approval can be found at: https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

Duration

14. The RIPA authorisation **must be reviewed or renewed in the time stated or cancelled** once it is no longer needed. Authorisation to carry out Directed Surveillance lasts for 3 months from authorisation. Authorisation to carry out CHIS lasts 12 months from authorisation .However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the authorisation is 'spent'. In other words, **the authorisation does not expire!** The authorisation has to be reviewed, renewed and/or cancelled once it is no longer required.
15.
16. Cancellation will need to be approved by the Chief Executive or Chief Operating Officer and is required whether the surveillance is conducted or the time period is due to lapse.

17. Magistrate's approval is required to renew an authorisation. There is no requirement for Magistrates to consider either cancellations or internal reviews.

18. Notices/Authorities issued under s22 compelling disclosure of communications data are only valid for one month, but can be renewed for subsequent periods of one month, at any time. Again, Magistrate's approval will be required for a renewal.

19. Authorisations can be renewed in writing before the maximum period in the Authorisation has expired. 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. Magistrate's approval will then be required.

20. An Authorisation cannot be renewed after it has expired. In such event, a fresh application will be necessary.

H. WORKING WITH / THROUGH OTHER AGENCIES

1. When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this Policy and the Home Office approved application forms must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be explicitly made aware what they are authorised to do.

2. When another agency (e.g. Police, DWP, Trading Standards, etc):-

   (a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the Council's record (a copy of which must be passed to the RIPA Co-ordinating Officer for the Central Register) or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

   (b) wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, the Council does not require its own RIPA form as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

3. In terms of 2(a) above, if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

4. **If in doubt, please consult with the SRO or the RIPA Co-ordinating Officer at the earliest opportunity.**

I. RECORD MANAGEMENT

1. **The Council must keep a detailed record of all Authorisations, Reviews, Renewals, Cancellations and Rejections for each respective service area. A Central Register of all Authorisation Forms will be maintained and monitored by the RIPA Co-ordinating Officer. All original forms (Authorisation, Review, Renewal, Cancellation) must be sent to the RIPA Co-ordinating Officer as soon as practicable.**

2. **Records maintained in the Service Area**

   The following documents must be retained by the relevant Head of Service (or their designated administrator) for such purposes:

   - a copy of all RIPA forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
   - a record of the period over which the surveillance has taken place;
   - the frequency of reviews prescribed by the Authorising Officer;
   - a record of the result of each review of the authorisation;
   - a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
   - the date and time when any instruction was given by the Authorising Officer; and
   - the Unique Reference Number for the authorisation (URN).

Central Register maintained by the RIPA Co-ordinating Officer

3. Each form will have a unique reference number (URN). The RIPA Co-ordinating Officer will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the forms for audit purposes. Rejected Forms will also have URN's.

4. Authorising Officers must forward a copy of every completed RIPA form to the RIPA Co-ordinating Officer for the Central Register, within 1 week of the Authorisation, Review, Renewal, Cancellation or Rejection. The RIPA Co-ordinating Officer will monitor the same and give appropriate guidance, from time to time, as necessary.

5. The Council will retain records for a period of at least three years from the ending of the Authorisation. The Office of Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual Authorisations, Reviews, Renewals, Cancellations and rejections.

J. CONCLUDING REMARKS

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Policy, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this Policy will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. **Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to consider a RIPA form. They must never sign or rubber stamp forms without thinking about their own personal and the Council's responsibilities.**

4. **Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same.** Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

5. For further advice and assistance on RIPA, please contact the SRO or the RIPA Co-Ordinating Officer.

APPENDIX 1 – LIST OF AUTHORISING OFFICER POSTS*

Assistant Director, Residents & Business

Assistant Director, Operations, Regulation and Enforcement

*This list is subject to update following structural changes at the council at the direction of the Chief Executive, Chief Operating Officer or Monitoring Officer.

*The Authorising Officer must be independent from the service submitting the request

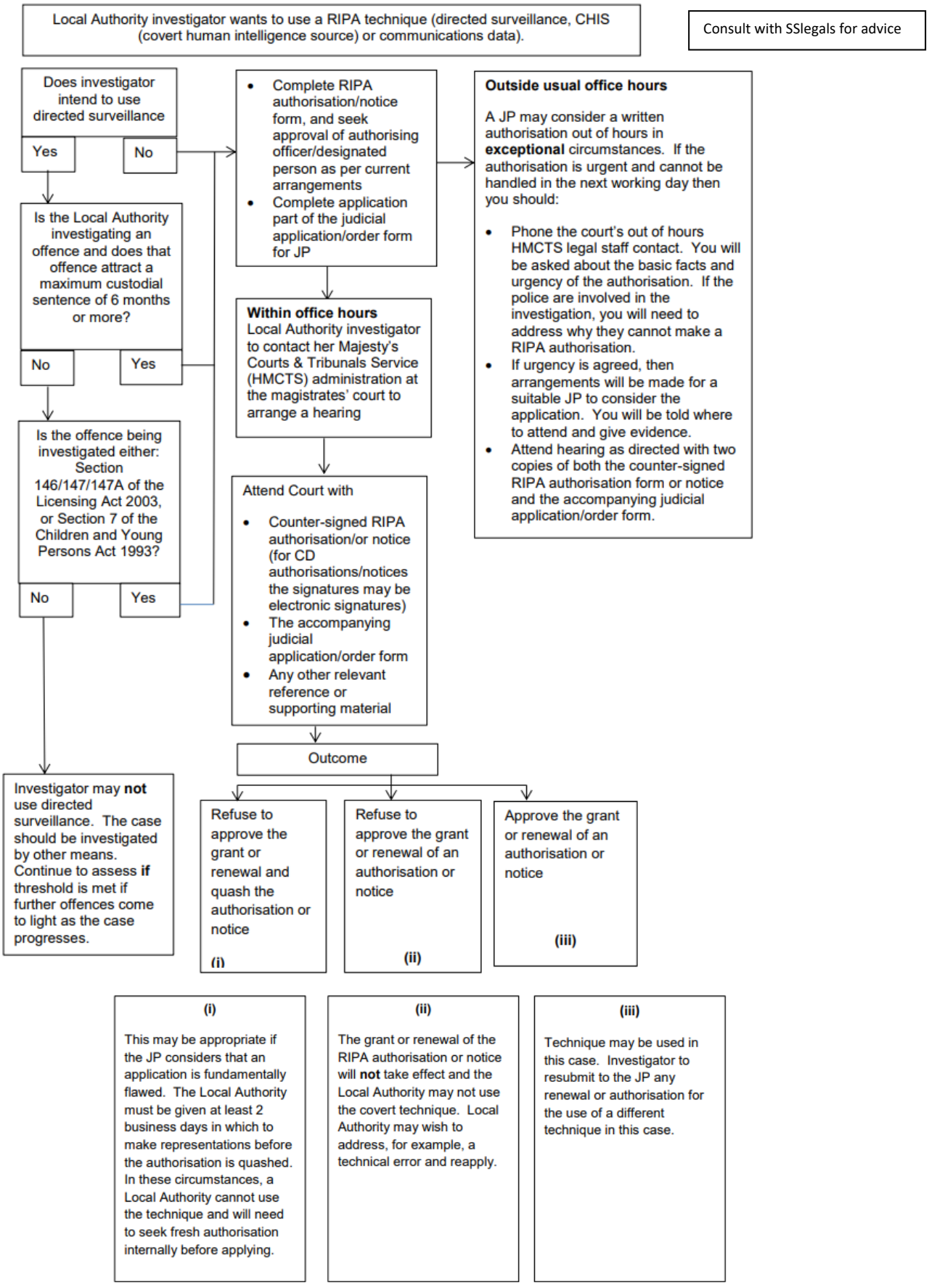
APPENDIX 2 - RIPA TRAINING, UPDATES AND REMINDERS

Training for staff will take place as and when necessary.

RIPA legislation guidance will be sent to all staff every 12 months. This will include updates where available.

Training for Authorising Officers take place on an annual basis. Additional training will be available when changes to legislation occur which impact their roles.

APPENDIX 3 – Magistrate's Court Authorisation Procedure



This page is intentionally left blank

AUDIT & MEMBER STANDARDS COMMITTEE WORK PROGRAMME FOR 2022/23

Item	21 July 2022	21 Sept 2022	30 Nov 2022	2 Feb 2023	23 Mar 2023	19 April 2023	Comments
FINANCE							
Annual Treasury Management Report	√						
Mid-Year Treasury Management Report			√				
Accounting Policies and Estimation Uncertainty						√	
Statement of Accounts			√*				*Dependent on when External Auditors complete the audit and issue their opinion. The deadline for 2021/22 accounts is 30 November. It is proposed that this will change to 30 September 2022 for the financial years 2022/23 to 2027/28 to match the next External Audit contract period.
Treasury Management Statement and Prudential Indicators				√			
Audit & Member Standards Committee Practical Guidance*							*Only relevant if there is updates to guidance so may not be needed
CIPFA Financial Management Code*							*Only relevant if there is updates to guidance so may not be needed
CIPFA Resilience Index	√						
Local Audit Update*							*Only relevant if there is updates to guidance so may not be needed
Overview of the Council's Constitution in respect of Contract and Financial Procedure Rules*							*Only relevant if there is updates to guidance so may not be needed
Annual report on Exceptions and Exemptions to Contract Procedure Rules 2021/22	√*						*Will be circulated as a briefing paper
INTERNAL AUDIT							
Chair of the Audit Committee's Annual Report to Council						√	
Annual Report for Internal Audit (including year-end progress report)						√	
Internal Audit Plan, Charter & Protocol 2023/24						√	

AUDIT & MEMBER STANDARDS COMMITTEE WORK PROGRAMME FOR 2022/23

Internal Audit Progress Report	√		√	√		*	*Included in the 'Annual Report for Internal Audit'
Review of the Effectiveness of the Audit & Member Standards Committee						√	
Quality Assurance and Improvement Programme /Public Sector Internal Audit Standards	√						
Risk Management Update	√		√	√		√	
Counter Fraud Update Report including Counter Fraud & Corruption/Whistleblowing/Anti-Money Laundering/ Prevention of Tax Evasion Policies			√				
GOVERNANCE & PERFORMANCE							
Annual Governance Statement						√	
GDPR/Data Protection Policy			√				
Annual Report of the Monitoring Officer – Complaints		√*					*To be circulated as a briefing paper
The Annual letter for Lichfield District Council from the Local Government Ombudsman			√*				*Potentially circulated as a briefing paper
RIPA reports policy and monitoring		√					
Terms of Reference							
EXTERNAL AUDITOR							
Audit Findings Report for Lichfield District Council 2021/2022			√*				*This will depend on when the External Auditors complete the audit and issue their opinion. The deadline for 2021/22 accounts is 30 November 2022.
The Annual Audit report for Lichfield District Council for 2021/22			√				
Audit Plan (including Planned Audit Fee 2022/23)						√	
Informing the Audit Risk Assessment - Lichfield District Council						√	
Audit Committee LDC Progress Report and Update – Year Ended 31 March 2023				√			

AUDIT & MEMBER STANDARDS COMMITTEE WORK PROGRAMME FOR 2022/23

Private meeting with the Internal and External Auditors		√		√		√	

This page is intentionally left blank