



## **Audit Committee Agenda**

**Wyre Borough Council**  
**Date of Publication: 2 November 2015**  
**Please ask for : Carole Leary**  
**Democratic Services Officer**  
**Tel: 01253 887444**

**Audit Committee meeting on Tuesday, 10 November 2015 at 6.00 pm  
in the Civic Centre, Poulton-le-Fylde**

- 1. Apologies for absence**
- 2. Declarations of interest**  

Members will disclose any pecuniary and any other significant interests they may have in relation to the matters under consideration.
- 3. Confirmation of minutes** (Pages 1 - 4)  

To approve as a correct record Minutes of the last meeting of the Audit Committee held on Tuesday 22 September 2015.
- 4. Review of Audit Committee's Performance** (Pages 5 - 10)  

Report of the Corporate Director of Resources.
- 5. Internal Audit and Risk Management - Progress Report** (Pages 11 - 26)  

Report of the Corporate Director of Resources
- 6. Annual Review of Council's Counter Fraud Policies - Anti Fraud, Corruption and Bribery, Whistle Blowing, Anti Money Laundering and Gifts and Hospitality and Registering Interests** (Pages 27 - 30)  

Report of the Corporate Director of Resources.
- 7. Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)** (Pages 31 - 62)  

Report of the Corporate Director of Resources
- 8. Annual Audit Letter 2014/15** (Pages 63 - 70)  

Report of the Corporate Director of Resources

**9. Items for Information**

(Pages 71 - 72)

Consultation on 2016/17 Work Programme and Scales of Fees

**10. Time and Date of Next Meeting**

Tuesday 8 March 2016 at 6pm, in Committee Room 1.



## Audit Committee Minutes

Minutes of the meeting of the Audit Committee of Wyre Borough Council held on Tuesday 22 September, 2015 at the Civic Centre, Poulton-le-Fylde.

---

### Audit Committee members present:

Councillor R Amos	Councillor Jones
Councillor Ballard	Councillor McKay
Councillor Barrowclough	Councillor Moon
Councillor Collinson	Councillor A Turner
Councillor Fail	Councillor Wilson
Councillor Greenhough	

**Apologies:** Councillors' E Anderton, Holden and Ingham and J Burrows – KPMG External Auditors

### Officers present:

P Davies – Corporate Director of Resources  
J Billington – Head of Governance  
H Rawding – Head of Finance  
C James – Financial Services Manager  
P Harrison – Financial Services Manager  
K McLellan – Senior Auditor  
C Leary – Democratic Services Officer

### Non-members present:

T Cutler – KPMG External Auditors and Councillor I Amos

**Members of the public present:** None

---

### AUDIT. 17 WELCOME AND APOLOGIES OF ABSENCE

The Chairman welcomed everyone to the meeting of the Audit Committee.

Apologies as detailed above.

### AUDIT. 18 DECLARATIONS OF INTEREST

None.

### AUDIT. 19 CONFIRMATION OF MINUTES

The minutes of the Audit Committee meeting held on Tuesday 30 June 2015 were confirmed as a correct record.

## **AUDIT. 20 STATEMENT OF ACCOUNTS 2014/15 (POST AUDIT)**

The Corporate Director of Resources submitted a report seeking Audit Committee's approval of the Council's published Statement of Accounts, following the completion of the audit, for the financial year 2014/15. The Audit Committee had approved the unaudited accounts for the 2014/15 financial year at their meeting on 30 June 2015. Following approval, the Statement of Accounts would be signed, dated and published on the web site, no later than 30 September 2015.

**RESOLVED** that approval be given to the Council's published Statement of Accounts for 2014/15.

## **AUDIT. 21 MANAGEMENT REPRESENTATION LETTER 2014/15**

The Corporate Director of Resources introduced the Management Representation Letter, the content of which is determined by KPMG. The letter would be signed by the Chairman of Audit Committee and the Chief Financial Officer, prior to it being sent to KPMG, the Council's External Auditors.

**RESOLVED** that the Management Representation Letter for 2014/15, signed by the Chairman of the Audit Committee and the Chief Financial Officer be sent to KPMG.

## **AUDIT. 22 REPORT TO THOSE CHARGED WITH GOVERNANCE (ISA 260) 2014/15**

Tim Cutler, a partner from the Council's external auditors (KPMG LLP (UK)) summarised the work that had been carried out to discharge their statutory audit responsibilities.

He provided Members with an overview of the report, summarising the headline messages for the Authority and key findings, namely;

- They anticipate issuing an unqualified audit opinion on the Authority's financial statements by 30 September 2015.
- They will report that the Annual Governance Statement complies with guidance issued by CIPFA/SOLACE.
- There were no unadjusted audit differences.
- A small number of presentational adjustments were required in relation to the audit fee, related parties and plant, property and equipment.
- The Authority has good processes in place for the production of the accounts and good quality supporting working papers.

Tim went on to say that there was a strong control environment in place at Wyre and as auditor's, they were confident that Wyre had cost improvement plans in place. He recognised the good work of the Finance Team and thanked officers for dealing promptly and efficiently with audit queries.

**RESOLVED** that the External Auditors Report to those charged with Governance, referred to as the ISA 260, for 2014/15, be noted.

## **AUDIT. 23 FINANCIAL REGULATIONS AND FINANCIAL PROCEDURE RULES – ANNUAL REVIEW**

The Corporate Director of Resources introduced the report and explained that the Financial Regulations and Financial Procedure Rules are reviewed annually, in accordance with best practice guidance.

The evidence of the regular review helps the Council demonstrate that it has put arrangements in place to maintain a sound system of internal control.

The Corporate Director of Resources referred to the proposed amendments listed in paragraph 5.1 of the report.

**RESOLVED** that the proposed changes to the Financial Regulations and Financial Procedure Rules – Annual Review are noted and approved.

## **AUDIT. 24 INTERNAL AUDIT CHARTER**

The Head of Governance introduced the report, explaining that the agreement of the Internal Audit Charter for the Audit and Risk Management Section ensuring compliance with the Public Sector Internal Audit Standards (PSIAS) is a requirement that came into force on 1 April 2013, superseding CIPFA's Code of Practice for Internal Audit in Local Government.

In response to a question from Councillor Fail, Joanne confirmed that the processes were regularly reviewed as part of the delivery of the audit plan and the completion of individual audits.

**RESOLVED** that the Internal Audit Charter and Code of Ethics be agreed.

## **AUDIT. 25 ANNUAL REVIEW OF THE RISK MANAGEMENT POLICY**

The Senior Auditor introduced the report, explaining the benefits of the Council's Risk Management approach, and indicated there had been no significant amendments to the Risk Management Policy. The Risk Register is available to view on the intranet along with the proposed actions to mitigate the risks.

The aim of the Risk Management Policy is to establish and operate an effective system, not only to minimise risk but to also enable continuous improvement at every level of the organisation. Members were informed that the Council's approach to risk management is key and the registers are updated at least every six months. The Audit Committee are asked to review the Risk Management Policy every year and the last review was completed in August 2014.

In response to a question from Cllr Moon about asylum seekers and Syrian refugees, Philippa reiterated that whilst Wyre are in discussions with DCLG regarding the process for accommodating asylum seekers, further advice is awaited about the co-ordinated response for refugees.

In response to a question from Cllr Turner about volumes of data, Joanne referred to data sampling software and techniques that were available to auditors to help focus their limited audit resource.

In response to a question from Cllr Fail, Joanne confirmed that officers were encouraged to review risk actions plans more frequently than six monthly and that risk ratings were regularly reviewed. She went on to say that risk identification was everyone's responsibility – employees, managers and elected members.

**RESOLVED** that the Annual Review of the Risk Management Policy document be approved.

**AUDIT. 26      REVISION OF THE 2015/16 AUDIT PLAN**

The Head of Governance introduced the report explaining why the plan required revision and seeking member's approval for the inclusion of the Information Governance work.

**RESOLVED** that the revised annual Audit Plan for 2015/16 be approved.

**AUDIT. 27      TIME AND DATE OF NEXT MEETING**

**Audit Committee Meeting, Tuesday 10 November at 6pm in Committee Room 1**

**AUDIT. 28      PERIODIC PRIVATE DISCUSSION WITH EXTERNAL AUDITORS**

Audit Committee members were given the opportunity to speak to the External Auditor in confidence, in accordance with the Audit Committee work programme.

*The Corporate Head of Resources, Head of Governance, Senior Auditor, Head of Finance and both Financial Services' Manager's and the Democratic Services Officer left the room for this item.*

The meeting started at 6pm and finished at 6.48pm

**Date of Publication: Tuesday 29 September, 2015**

arm/audit/mins/220915

Report of:	Meeting	Date	Item No.
Corporate Director of Resources (S.151 Officer)	Audit Committee	10 November 2015	4

<b>Review of Audit Committee's Performance</b>
--

**1. Purpose of report**

1.1 To consider CIPFA's Self-Assessment of Good Practice contained within the CIPFA publication 'Audit Committees: Practical Guidance for Local Authorities and Police 2013' and identify the actions necessary to ensure that the Audit Committee meets best practice guidance and provides value to the authority.

**2. Outcomes**

2.1 The determination of an improvement plan.

**3. Recommendation**

3.1 That the Audit Committee considers CIPFA's Self-Assessment of Good Practice at Appendix 1 and agree those areas where further improvement is considered beneficial.

**4. Background**

4.1 Audit committees are a key component of an authority's governance framework. Their function is to provide an independent and high-level resource to support good governance and strong public financial management.

4.2 An Audit Committee's effectiveness should be judged by the contribution it makes to, and the beneficial impact it has on the authority's business.

4.3 Evidence of effectiveness will usually be characterised as 'influence', 'persuasion' and 'support'. A good standard of performance against recommended practice, together with a knowledgeable and experienced membership, are essential for delivering effectiveness.

**5. Key issues and proposals**

5.1 Authorities are encouraged not to regard meeting the recommended practice as a tick box activity and are reminded that achieving recommended practice does not mean necessarily that the committee is effective. To help give a more rounded opinion of the committee's

effectiveness, further guidance has been provided in the publication in respect of a knowledge and skills framework which can be used to guide members on their training needs.

**5.2** At the last review in November 2014 it was decided that the Head of Governance would hold one-to-one meetings with each member of the Audit Committee to discuss the self-assessment and document suggested improvements, however due to the number of new Audit Committee members who have only attended 3 meetings to date, it was felt that it would be more beneficial to discuss the self-assessment at the meeting and to agree the proposed improvement plan.

**5.3** The self-assessment at Appendix 1 has been completed by the Head of Governance and ratified by the Corporate Director of Resources (Section 151 Officer). Members will be asked to contribute to a discussion at the meeting with a view to developing an agreed action plan.

<b>Financial and legal implications</b>	
Finance	There are no specific financial implications arising from the agreement of the improvement plan.
Legal	There are no specific legal implications arising from the agreement of the improvement plan.

#### **Other risks / implications: checklist**

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

<b>implications</b>	<b>✓ / x</b>
community safety	<b>x</b>
equality and diversity	<b>x</b>
sustainability	<b>x</b>
health and safety	<b>x</b>

<b>risks/implications</b>	<b>✓ / x</b>
asset management	<b>x</b>
climate change	<b>x</b>
data protection	<b>x</b>

report author	telephone no	email	date
Joanne Billington	01253 887372	Joanne.billington@wyre.gov.uk	23 October 2015

<b>List of background papers:</b>		
name of document	date	where available for inspection

#### **List of appendices**

Appendix 1 – CIPFA Self-Assessment of Good Practice

arm/audit/cr/15/1011jb2



## CIPFA self-assessment of Good Practice – November 2015

Good practice questions		Yes	Partly	No	Comments
<b>Audit committee purpose and governance</b>					
1	Does the authority have a dedicated audit committee?	✓			The Audit Committee has been in place since December 2005.
2	Does the audit committee report directly to full council? (Applicable to local government only.)	✓			<p>A periodic report is submitted to Full Council with the last report being considered September 2015.</p> <p><b>Action C/F: This will be amended to include additional information such as attendances.</b></p> <p><b>Completed and reflected in the September 2015 periodic report.</b></p>
3	Do the terms of reference clearly set out the purpose of the committee in accordance with CIPFA's Position Statement?	✓			<p><b>Action C/F: The Audit Committees terms of reference will be reviewed to include the purpose of the Audit Committee as documented in CIPFA's Position Statement.</b></p> <p><b>Agreed by Audit Committee March 2015 and reflected in the constitution updated 16 April.</b></p>
4	Is the role and purpose of the audit committee understood and accepted across the authority?	✓			The terms of reference are reviewed annually by the Committee in March and also form part of the Council's Constitution.
5	Does the audit committee provide support to the authority in meeting the requirements of good governance?	✓			The Audit Committee provide assurance on the adequacy of internal control, risk management and the integrity of financial reporting and the annual governance processes.
6	Are the arrangements to hold the committee to account for its performance operating satisfactorily?	✓			A review of effectiveness is completed annually.

Functions of the committee					
7	<p>Do the committee's terms of reference explicitly address all the core areas identified in CIPFA'S Position Statement?</p> <ul style="list-style-type: none"> <li>▪ good governance</li> <li>▪ assurance framework</li> <li>▪ internal audit</li> <li>▪ external audit</li> <li>▪ financial reporting</li> <li>▪ risk management</li> <li>▪ value for money or best value</li> <li>▪ counter-fraud and corruption</li> </ul>	✓			<p><b>Action C/F: Although the current terms of reference reflect the core functions of an Audit Committee, it will be rewritten to reflect the suggested terms of reference in the CIPFA guidance.</b></p> <p><b>Agreed by Audit Committee March 2015 and reflected in the Constitution updated 16 April.</b></p>
8	<p>Is an annual evaluation undertaken to assess whether the committee is fulfilling its terms of reference and that adequate consideration has been given to all core areas?</p>	✓			<p>The annual review of effectiveness gives the Audit Committee the opportunity to assess if it is fulfilling the terms of reference.</p> <p><b>Action C/F: A further assessment will be completed in November 2015 using the updated terms of reference (TOR). The suggested TOR will also be used to train new audit committee members from May 2015.</b></p> <p><b>Completed May 2015</b></p>
9	<p>Has the audit committee considered the wider areas identified in CIPFA's Position Statement and whether it would be appropriate for the committee to undertake them?</p>	✓			<p>The Audit Committee already participate by considering governance and risk. The Code of Practice on Treasury Management requires a body to be nominated and responsible for ensuring effective scrutiny of the Treasury Management Strategy and policies. The Council has nominated the Overview and Scrutiny Committee (Cabinet 25/03/2015).</p>
10	<p>Where coverage of core areas has been found to be limited, are plans in place to address this?</p>	N/A	N/A	N/A	<p>There have been no instances where coverage of core areas has been found to be limited.</p>
11	<p>Has the committee maintained its non-advising role by not taking on any decision-making powers that are not in line with its core purpose?</p>	✓			<p>The Committee does not take on any decision making powers that are not documented within its terms</p>

		Yes	Partly	No	of reference.
Good practice questions		Yes	Partly	No	
Membership and support					
12	<p>Has an effective audit committee structure and composition of the committee been selected? This should include:</p> <ul style="list-style-type: none"> <li>▪ separation from the executive</li> <li>▪ an appropriate mix of knowledge and skills among the membership</li> <li>▪ a size of committee that is not unwieldy</li> <li>▪ where independent members are used, that they have been appointed using an appropriate process.</li> </ul>	<p>✓ ✓ ✓ N/A</p>			<p>Whilst individual Members of the Audit Committee may also serve on overview and scrutiny the audit committee is independent of the scrutiny function. The Audit Committee Chairman is not a member of the Executive. Members have completed Councillor Development Plans, which have been evaluated and appropriate training sessions provided.</p> <p>The Cross-Party Councillor Development Group now meet quarterly to identify new training needs and the Member Development Officer arranges training as required.</p>
13	Does the chair of the committee have appropriate knowledge and skills?	✓			<p>The Audit Committee Chairman was recently appointed in May 2015.</p> <p><b>Action</b></p> <p><b>A one-to-one assessment will take place with the new Chairman, Head of Governance and the Section 151 Officer to ensure the Chairman has the appropriate Knowledge and skills in the following areas;</b></p> <ul style="list-style-type: none"> <li>• Finance</li> <li>• Treasury Management</li> <li>• Value for Money</li> <li>• Risk Management</li> </ul>
14	Are arrangements in place to support the committee with briefings and training?	✓			
15	Has the membership of the committee been assessed against the core knowledge and skills framework and found to be satisfactory?	✓			<p>Members have completed Councillor Development Plans, which have been evaluated and appropriate training sessions provided. The Cross-Party Councillor Development Group now meet quarterly to identify</p>

					<p>new training needs and the Member Development Officer arranges training as required.</p> <p>The induction training in May 2015 covered the core areas of the knowledge and skills framework. On-going Audit Committee attendance will ensure members complete the work programme thereby continually enhancing their knowledge and skills.</p>
16	Does the committee have good working relations with key people and organisations, including external audit, internal audit and the chief financial officer?	✓			
17	Is adequate secretariat and administrative support to the committee provided?	✓			
<b>Effectiveness of the committee</b>					
18	Has the committee obtained feedback on its performance from those interacting with the committee or relying on its work?			✓	<b>Action: Feedback will be sought annually from the External Auditor.</b>
19	Has the committee evaluated whether and how it is adding value to the organisation?	✓			<p><b>Action: Members will be asked to complete a questionnaire in respect of any qualifications, specific knowledge or experience they may have which may add value to the committee and/or the organisation. Questionnaires should be returned no later than 1 December 2015.</b></p> <p><b>The Head of Governance will email feedback from the exercise in December 2015.</b></p>
20	Does the committee have an action plan to improve any areas of weakness?	✓			Actions contained within this checklist are highlighted in bold and will be implemented prior to the next annual review.



Report of:	Meeting	Date	Item No.
Corporate Director of Resources (S.151 Officer)	Audit Committee	10 November 2015	5

<b>Internal Audit and Risk Management - Progress Report</b>
---

**1. Purpose of report**

1.1 To review progress in relation to Internal Audit and Risk Management and consider progress against the action plan resulting from the 2014/15 Annual Governance Statement.

**2. Outcomes**

2.1 Effective leadership of audit and governance issues allowing the Council to demonstrate that arrangements are in place to maintain a sound system of internal control.

**3. Recommendation**

3.1 Members are asked to note the progress reports attached at Appendices 1, 2, and 3.

**4. Background**

4.1 The Audit Committee has a clear role in relation to the authority's internal audit function and this involves:

- Formally approving, but not directing, the overall strategy to ensure that it meets the council's overall strategic direction;
- Approving the annual programme of audits (paying particular attention to whether there is sufficient and appropriate coverage); and
- Monitoring progress against the plan and assessing whether adequate skills and resources are available to provide an effective audit function.

4.2 The Audit Committee's role in relation to reviewing the work carried out will include formal consideration of summaries of work done, key findings, issues of concern and actions planned as a result of audit work. A key part of the role is receiving and reviewing regular reports from the Head of Governance in order to reach an overall opinion on the internal control environment and the quality of internal audit coverage.

## 5. Key issues and proposals

- 5.1 The progress reports in relation to Internal Audit, Risk Management and the action plan resulting from the 2014/15 Annual Governance Statement are attached at Appendices 1, 2, and 3.

<b>Financial and legal implications</b>	
Finance	The annual programme of audits is performed by the in house team supplemented by 70 audit days supplied by Lancashire Audit services and Mazars met by existing budgetary provision.
Legal	Effective audit and risk management assist in good governance and probity of Council actions.

### **Other risks / implications: checklist**

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

<b>implications</b>	<b>✓ / x</b>
community safety	<b>x</b>
equality and diversity	<b>x</b>
sustainability	<b>x</b>
health and safety	<b>x</b>

<b>risks/implications</b>	<b>✓ / x</b>
asset management	<b>x</b>
climate change	<b>x</b>
data protection	<b>x</b>

report author	telephone no	email	date
Joanne Billington	01253 887372	Joanne.billington@wyre.gov.uk	23 October 2015

<b>List of background papers:</b>		
name of document	date	where available for inspection

### **List of appendices**

Appendix 1 – Internal Audit Progress Report  
 Appendix 2 – Risk Management Progress Report  
 Appendix 3 – Annual Governance Statement 2014/15 - Action Plan update

arm/audit/cr/15/1011jb1

### INTERNAL AUDIT PROGRESS REPORT – MAY 2015 to OCTOBER 2015

#### THE AUDIT PLAN AND DELIVERY

The Internal Audit and Risk Management Section is responsible to the Corporate Director of Resources for carrying out a continuous examination of the accounting, financial and other operations of the Council in accordance with Section 151 of the Local Government Act 1972 and the Accounts and Audit Regulations 2015. The latter states that ***“the relevant body shall be responsible for ensuring that the financial management of the body is adequate and effective and that the body has a sound system of internal control which facilitates the effective exercise of that body’s functions and which includes arrangements for the management of risk.”***

Members of the Audit Committee should note that copies of internal audit reports are published on the Council’s Intranet. Access to the supporting files is available to members of the Audit Committee on request. The table overleaf summarises audit work performed since the last progress report in May 2015.

Wyre Council attends the Lancashire District Council’s Audit Group and continues to participate in the Audit Commissions National Fraud Initiative data sharing exercise. The Council also works closely with the Association of Local Authorities Risk Managers (ALARM) and our insurer, Zurich Municipal.

The annual contract with Lancashire Audit Services (LAS) provides 38 days of audit support at a rate of £260 per day for 2015/16. A further 32 days of audit support is completed by a private audit company ‘Mazars’ at the same rate. This is supplemented by work performed by the in house team. The work completed by the in-house team is benchmarked against the work carried out by LCC and Mazars to ensure that quality and standards are maintained.

All the major reviews conducted to date have been completed within or below the agreed time scales and to budget, and additional benefits continue to be derived from consultation with Lancashire Audit Services and Mazars, given their wealth of experience and extensive client base.

Internal Audit will continue to provide the Council with the necessary assurance about its various activities and associated systems, as outlined in the Council’s Internal Audit Charter.

## Audit Work Performed May to October 2015

As summarised below the following reviews have been performed and reports issued since the last progress report was delivered in the Annual Audit report in May 2015. Lancashire Audit Services and Mazars have not yet started any of the planned work from the 2015/16 audit plan, however work is due to commence in November.

### Wyre Council Reports

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
<b><u>Audit work from 2014/15 completed since May 2015</u></b>								
<b>Working Together With Families</b>	<b>Final Report Issued</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>Excellent</b>	The overall opinion of the auditor is that the controls in place to manage the funding received for the WTWF project are excellent. This means that controls are in place to ensure the achievement of service objectives, good corporate governance and to protect the Council / Partnership against significant foreseeable risks. Compliance with the risk management process is considered to be good and no significant or material errors or omissions were found. There were no recommendations made.
<b>Building Maintenance</b>	<b>Final Report Issued</b>	<b>2</b>	<b>10</b>	<b>6</b>	<b>2</b>	<b>0</b>	<b>Fair</b>	Areas have been identified where improvements could be made to strengthen the control environment, namely; <ul style="list-style-type: none"> <li>• The project management module on the Technology Forge system has not been developed;</li> <li>• Documented procedures and processes are not in place for all work undertaken by</li> </ul>



TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								<p>the Building Maintenance Team;</p> <ul style="list-style-type: none"> <li>• Departmental risk assessments are not reviewed annually and communicated to staff;</li> <li>• All job repairs are not completed in accordance with the timescales allocated;</li> <li>• A programme of planned maintenance has not been developed using the information contained in the condition surveys;</li> <li>• An inspection schedule showing the type of inspection and the due date has not been compiled;</li> <li>• A written agreement is not in place covering the inspection work undertaken by Lancashire County Council;</li> <li>• The terms and conditions of contract for the purchase of services are not signed when awarding a contract;</li> <li>• Current arrangements for the control of asbestos are not satisfactory;</li> <li>• Completed legionella inspection reports for all council buildings have not been received by the Building Maintenance Team;</li> <li>• The Civic Centre fire procedures are not routinely implemented;</li> <li>• Fixed electrical installation certificates are not held for all council properties;</li> <li>• The re-active maintenance framework agreement has not been working in accordance with the agreement;</li> <li>• Labour has not been charged in</li> </ul>

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								<p>accordance with the schedule of approved labour rates agreed in the reactive maintenance framework;</p> <ul style="list-style-type: none"> <li>• Goods and services are not always procured in accordance with the Financial Regulations and Financial Procedure Rules;</li> <li>• There is no interface between the Technology Forge system and the Civica purchasing system resulting in purchase orders not being raised;</li> <li>• Invoices are not approved in accordance with authorisation limits in all instances;</li> <li>• There are no procedures and processes in place to ensure compliance with the Construction (Design and Management) Regulations 2015;</li> <li>• An inspection policy has not been developed and where inspections are completed these are not documented; and</li> <li>• The annual and responsive maintenance budget was exceeded by £20,032 in 2014/15;</li> </ul>
<b>Street Scene - Area Officers</b>	<b>Final Report Issued</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>0</b>	<b>1</b>	<b>Good</b>	<p>Areas have been identified where improvements could be made to strengthen the control environment, namely;</p> <ul style="list-style-type: none"> <li>• Lunch breaks are not accurately recorded on the flexitime records;</li> <li>• Actions agreed at weekly briefings are not documented;</li> <li>• There was no evidence identified to</li> </ul>

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								<p>confirm that risk assessments are reviewed on an annual basis;</p> <ul style="list-style-type: none"> <li>• Spot checks of all public conveniences are not routinely completed;</li> <li>• Supervisory checks of the street cleansing and bin collection schedules are not completed every weekend;</li> <li>• The stock of Council dog microchips was found to be incorrect;</li> <li>• A record of donations made to the Dogs Trust are not recorded and in some instances are not banked promptly;</li> <li>• Procedures and processes are required to control the data collected whilst using the camera badges; and</li> <li>• No timescales have been agreed for the procurement exercise to be undertaken for the kennelling contract.</li> </ul>
<b><u>2015 / 16 Audit work</u></b>								
<b>Housing Options - Homelessness</b>	<b>Final Report Issued</b>	<b>0</b>	<b>4</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>Good</b>	<p>Areas have been identified where improvements could be made to strengthen the control environment, namely;</p> <ul style="list-style-type: none"> <li>• The revised Homelessness Strategy completed in 2014 has not been formally accepted or published;</li> <li>• All of the documented procedures completed in 2009 have not been reviewed and updated;</li> <li>• Case file reviews are not signed off by a</li> </ul>

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								<p>Senior Officer in all instances;</p> <ul style="list-style-type: none"> <li>Data sharing agreements have not been established;</li> <li>Paper and electronic files are not routinely destroyed in accordance with the storage and retention policy;</li> <li>The phone ahead fax policy is not documented;</li> <li>Evidence of valid fire certificates and public liability insurance has not been requested for bed and breakfast accommodation;</li> <li>No evidence is held that the risk assessments have been communicated to staff;</li> <li>The spreadsheets for the DHIS and Landlord incentive schemes do not accurately reflect current expenditure; and</li> <li>Purchase orders are not raised for the goods and services requested by the Housing Options Service.</li> </ul>
<b>Waste Contract and Monitoring arrangements – Follow up</b>	<b>Final Report Issued</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>Excellent</b>	<p>Areas have been identified where improvements could be made to strengthen the control environment, namely;</p> <ul style="list-style-type: none"> <li>Procedures are required to control the data collected through the use of 360 degree cameras; and</li> <li>Supervisory audits are not completed equally by the council for all rounds or</li> </ul>

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								documented in all instances.
<b>Fleetwood and Poulton Market</b>	<b>Draft Report Issued</b>							The overall objective of the audit is to examine the adequacy and effectiveness of controls in place around Fleetwood and Poulton Market. The terms of reference can be reviewed on BRIAN under the Audit and Risk Management webpages.
<b>Regulation of Investigatory Powers Act (RIPA)</b>	<b>Fieldwork in progress</b>							The overall objective of the audit is to examine the adequacy and effectiveness of controls in place around compliance to RIPA. The terms of reference can be reviewed on BRIAN under the Audit and Risk Management webpages.
<b>CCTV – Compliance with Code of Practice</b>	<b>Fieldwork in progress</b>							The overall objective of the audit is to examine the adequacy and effectiveness of controls in place around compliance to the CCTV Code of Practice. The terms of reference can be reviewed on BRIAN under the Audit and Risk Management webpages.
<b>Rossall Sea Defences</b>	<b>Fieldwork in progress</b>							No report will be issued for this piece of work. Fieldwork to date has included; attending project board meetings, reviewing risk registers and examining the contracts terms and conditions. It is felt that a continual review is more beneficial to the Head of Engineering allowing advice and assistance to be provided at the time it is required rather than after the event.  To date, the auditor has no major concerns that

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								<p>need to be raised with the Section 151 Officer which would have an adverse effect on the Annual Governance Statement; however at the last project board meeting it was identified that the Anchorsholme scheme has passed its contract completion date which results in the contractor incurring all expenditure on further works. The Head of Engineering and the Project Manager have been advised to monitor on-going costs to ensure expenditure is correctly attributable to the Rossall Scheme.</p>

## **Other audits to be performed in 2015/16 (ending 31 March 2016)**

### Wyre Council Reports

- YMCA (10 days)
- Thornton Little Theatre (5 days)
- E-Benefit System (5 days)
- Private Sector Housing – Grants and Enforcement (10 days)
- Compliance to Anti-social Behaviour, Crime and Policing Act 2014 (10 days)

### LCC Reports

- Debtors, Creditors and Budgetary Control (20 days)
- Treasury Management (10 days)
- Housing benefit Overpayments (5 days)

### Mazars Reports

- Follow up work from 2014/15 Audit Plan (10 days)
- Development Control (10 days)
- Care and Repair (10 days)

### Changes to the 2015/16 Audit Plan

The Audit Plan for 2015/16 has been amended to allow the Senior Auditor to carry out 45 days' work on completing the actions reported following the Information Governance audit in January 2015. The following audits have been rolled to 2016/17 to allow work to commence;

- Compliance to Financial Regulations
- Committee Reports – Implications and Reporting Deadlines
- Compliance to Public Internal Audit Standards.

## **Other audit work undertaken:**

### Investigations

All whistleblowing calls and investigations carried out are logged and investigated with the confidential outcomes being reported to the Audit Committee's Chairman and Vice Chairman and also to the Councils external Auditor, KPMG. To date, there have been no whistleblowing calls during 2015/16 that have required internal audit investigation.

### National Fraud Initiative – Audit Commission's data matching exercise.

Data has been uploaded to the Audit Commissions secure data matching system. The matches were realised in January 2015 and officers are in the process reviewing the matches identified. A report will be produced once the outcomes of the data matching exercise have been completed.

### Gifts and Hospitality

The gifts and hospitality register is continually maintained throughout the year and is monitored by both the Council's Monitoring Officer and the Audit Committee. The register was examined by the Audit Committee in May 2014 and by the Monitoring Officer in December 2014.

A reminder has been placed in Novembers Core Brief, reiterating to staff the importance of declaring all gifts and hospitality received and that there is now an on-line form on BRIAN to facilitate the reporting process. Since April 2015 there has been 9 declarations made by council officers receiving gifts and hospitality.

### Information Governance

The Council's on-line training package - 'Focus on Information Security' has been completed by all staff. All new starters are required to complete and pass the course within four weeks of their start date. It has now been rolled out to all new members; however there are still x long-standing members who have yet to complete the training package.

As detailed above, work is about to commence in implementing the actions highlighted in Lancashire Audit Services report on the Council's Information Governance framework. 45 audit days has been allocated to implement information asset registers. The registers will show the data's classification, the asset owner and also the storage and retention requirements.

### Follow-up Reviews

Mazars have been commissioned to carry out an annual follow-up review of all recommendations made during the audit year. A sample of recommendations (Level 1-3) are selected at random and officers are contacted to seek assurance that they have been implemented.

### Security Sweeps

A security sweep of the Civic Centre was carried out in October 2015. No major concerns were identified and all minor issues have been reported to Heads of Service to ensure they are resolved with the individual officers concerned.

### Anti-Fraud and Corruption Awareness

The councils counter fraud policies are reviewed annually in November and are approved by the Audit Committee. A refresher exercise will be completed before March 2016 to test awareness of existing staff and also pick up any new starters to the Council who may not have had the opportunity to read the polices provided to them as part of their induction.



### **RISK MANAGEMENT PROGRESS REPORT**

#### **Operational Risks**

Progress on the embedding of risk management is reported to the Audit Committee via six monthly reports by the Head of Governance (Chief Internal Auditor). This is in line with the Council's Risk Management Policy, originally approved by Cabinet in April 2004 and reviewed and approved annually by the Audit Committee in August.

Risk workshops are held in April each year with each service unit identifying any new risks that may occur during the year preventing the achievement of individual service plans. It is also an opportunity to review progress made in respect of any existing risks, remove risks that are no longer valid and action plan to mitigate against identified risks wherever possible.

All staff who have responsibilities for identified risks are encouraged to review their risks and update their action plans continually throughout the year, however a prompt is issued to staff in October to ensure progress is documented.

The Council is currently using spreadsheets to assist with the management of operational risks and these can be viewed by following the link below. The Audit Committee are encouraged throughout the year to go and view the risks identified by each service unit and ensure progress is being made to mitigate each risk and challenge officers in the instances where no progress has been made.

<http://intranet/services/RiskManagement/Pages/default.aspx>

#### **Strategic Risks**

The Council's strategic risk register is reviewed every six months. Any changes to the ratings are documented and supported by a valid reason and sufficient evidence. The 6 monthly review was carried out with the Corporate Management Team on the 29 October 2015 and the results will be reported verbally to the Audit Committee.

The next strategic risk workshop will be held on the 7 March 2016.

**ANNUAL GOVERNANCE STATEMENT 2014/15 – ACTION PLAN UPDATE**

<b>Governance Issues</b>	<b>Risk Rating</b>	<b>Year relating to</b>	<b>Actions</b>	<b>Responsible Officer</b>	<b>Position at October 2015</b>
<b>Information Governance</b>	Medium	2014/15	A review of the Council's Information Governance procedures in January 2015 highlighted that the Council does not hold a data asset register. Whilst the Council is in the process of identifying all of its data assets (both electronic and paper) for the purpose of the corporate retention schedules, the audit advised that the retention schedules are modified to include a data classification scheme and named data asset owners.	J Billington	45 days have been assigned to modify the format of the current retention schedules and then roll out to all services. Once an asset classification scheme has been identified, the Senior Auditor will attend HOS team briefs to identify asset owners.
Page 24	Medium	2013/14	Elected Members, as data Controllers in their own rights, need to understand and comply with the 8 data protection principles. The FOCUS on information Security eLearning test will be rolled out to all members, each member will be asked to register as a Data Controller with the Information Commissioner and postcards will be issued to members making simple the key points to Data Protection.	J Billington	There are still a number of elected members that have yet to complete the data security training. The licence for the FOCUS training package has now expired, however a new training tool has been sourced from the Civil Service. This will now be used for all members who have not yet completed any training.
<b>Health &amp; Safety</b>	High	2014/15	In October 2014 the Health and Safety Advisor identified a number of weaknesses in respect of the management of asbestos. An action plan to address the weaknesses was drawn up, however a review in March 2015 identified that the necessary action had not been taken. It was agreed following an internal audit in July 2015 that the current asbestos register for each building will be reviewed and updated and	M Blundy / J Holden	The Building Maintenance Team (BMT) are continuing to use the existing asbestos risk assessments. Risk assessments have been commissioned from LCC for all buildings that the council operates.

			the Managers of each building will be informed of the procedures to be completed.		Following completion of the new risk assessments the asbestos registers will be updated and revised procedures to building managers will be rolled out. Asbestos training has also been completed by the BMT in October 2015.
<b>Democratic Services</b>	Medium	2014/15	The interim arrangement with Blackpool and Fylde in relation to the Council's Independent Person has been terminated. New arrangements will need to be made.	R.Saunders	A new Independent Person has been appointed at Wyre and an agreement to share the Independent Person at South Ribble is now in place.

This page is intentionally left blank



Report of:	Meeting	Date	Item No.
Corporate Director of Resources (S.151 Officer)	Audit Committee	10 November 2015	6

**Annual Review of Council's Counter Fraud Policies - Anti Fraud, Corruption and Bribery, Whistle Blowing, Anti Money Laundering and Gifts and Hospitality and Registering Interests**

## 1. Purpose of report

### 1.1 Approval of the Council's Counter Fraud Policies, namely:

- Anti-Fraud, Corruption and Bribery;
- Anti-Money Laundering;
- Whistleblowing; and
- Gifts and Hospitality and Registering Interests.

## 2. Outcomes

2.1 The ability to demonstrate that the Council has arrangements in place that are designed to promote and ensure probity and propriety in the conduct of its business.

## 3. Recommendation

3.1 Members are asked to approve the policy documents detailed above which are published on the Council's intranet.

## 4. Background

4.1 The Audit Committee work plan includes an annual review of the following policies:

Anti-Fraud, Corruption and Bribery - originally approved by the Standards Committee in 2006. The policy was amended in November 2011 to make reference to the Bribery Act 2010, which came into effect on the 1 July 2011.

Anti-Money Laundering - first introduced in 2007 to comply with the new 'Money Laundering Regulations 2007 Act', which came into effect in December 2007.

Whistleblowing - originally agreed by the Standards Committee in 2004. The whistleblowing policy has been reviewed using the British Standards Institute (BSI) Whistleblowing Arrangements Code of Practice for 1998:2008 and the Enterprise and Regulatory Reform Act (ERRA) which received royal assent on 25 April 2013. The ERRA includes major changes to employment law which will impact considerably on whistleblower protection. The policy has also been reviewed to ensure it is in line with the Public Concern At Work publication; The Whistleblowing Commission - Report on the effectiveness of existing arrangements for workplace whistleblowing in the UK, published in November 2013.

Gifts and Hospitality and Registering Interests – originally agreed by Audit Committee in February 2009.

## 5. Key issues and proposals

- 5.1 The general aim of all the Council’s counter fraud policies is to reduce the occurrence and impact of fraud, corruption and bribery on the organisation and provide an effective channel of communication for anyone who has concerns or suspicions of malpractice.
- 5.2 The Whistleblowing Policy has been amended to show the Councils dedicated Whistleblowing telephone number and email address.
- 5.3 The Anti-Money Laundering Policy and Procedures has been amended to show that the Serious Organised Crime Agency (SOCA) is now known as the National Crime Agency (NCA).
- 5.4 The Anti-Fraud, Corruption and Bribery Policy has been amended to reflect that the Benefit Fraud Team is now the Compliance Team.
- 5.5 There have been no changes made to the Gifts and Hospitality and Registering Interests policy.

All the policies can be viewed by clicking on the following link;

<http://intranet/services/Counter%20Fraud%20and%20Corruption/Pages/default.aspx>

<b>Financial and legal implications</b>	
Finance	There are no specific financial implications arising from the adoption of these counter-fraud policies.
Legal	The Councils counter-fraud policies assist in good governance and probity of Council actions and decision-making. Whilst there is no statutory requirement to comply with the money laundering regulations, the Audit Commission believes that Councils should comply with the spirit and principle of the legislation. An effective Anti-Money Laundering Policy and associated training will help to ensure that Council complies with the money

	Laundering Regulations, the Proceeds of Crime Act and similar legislation.
--	--

**Other risks / implications: checklist**

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

<b>implications</b>	<b>✓ / x</b>
community safety	<b>x</b>
equality and diversity	<b>x</b>
sustainability	<b>x</b>
health and safety	<b>x</b>

<b>risks/implications</b>	<b>✓ / x</b>
asset management	<b>x</b>
climate change	<b>x</b>
data protection	<b>x</b>

report author	telephone no	email	date
Joanne Billington	01253 887372	Joanne.billington@wyre.gov.uk	20 October 2015

<b>List of background papers:</b>		
name of document	date	where available for inspection

**List of appendices**

arm/audit/cr/15/1011jb3

This page is intentionally left blank





Report of:	Meeting	Date	Item No.
Corporate Director of Resources	Audit Committee	10 November 2015	7

## Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)

### 1. Purpose of Report

- 1.1 To review the authority's use of RIPA since it was last considered at the Audit Committee in November 2014.
- 1.2 To perform the annual review of the Council's Policy.

### 2. Outcomes

- 2.1 Evidence that the Council complies with current legislation.

### 3. Recommendations

- 3.1 Members are requested to note that there has been no use of the Council's powers to conduct directed surveillance under the Regulation of Investigatory Powers Act 2000.
- 3.2 Members are requested to agree the revised policy attached at Appendix One which reflects minor amendments.

### 4. Background

- 4.1 Local authorities can undertake surveillance and access communications data under the framework of the Regulation of Investigatory Powers Act 2000. These rules set high standards for all public authorities that use these powers to undertake a range of enforcement functions to ensure they can keep the public safe and bring criminals to justice, whilst protecting individuals' rights to privacy.
- 4.2 Members will recall that from 1 November 2012, the Protection of Freedoms Act 2012 (the Act) became effective. It introduced a more restrictive approach to the use of RIPA by local authorities by limiting the use of direct authorisations to serious crimes, i.e. those crimes punishable by a maximum custodial sentence of 6 months or more or

those constituting an offence of selling alcohol or tobacco to children. The application must also have judicial approval by a magistrate before an authorisation takes effect and the magistrate needs to be satisfied that there are reasonable grounds for believing that the requirements of RIPA are met.

## **5. Key Issues and Proposals**

- 5.1** The Code of Practice requires a number of best working practices to be adopted by all public authorities, including:
- An annual review of the authority's use of RIPA to ensure that it is being used consistently and in accordance with the Council's policy; and
  - An annual review of the policy ensuring that it remains fit for purpose.
- 5.2** There is a requirement for the Council to nominate a Senior Responsible Officer, who will be responsible for:
- The integrity of the RIPA process in place within the Council to authorise surveillance and the covert use of human intelligence source (CHIS);
  - Compliance with the legislation and codes of practise;
  - Engagement with the Commissioners and inspectors when they conduct their inspections; and
  - Overseeing the implementation of any post inspection action plan recommended by the Commissioner.
- 5.3** There is also a requirement to have a Senior Responsible Officer who oversees the competence of authorising officers and the processes in use in the authority. Both of these roles are allocated to the Senior Solicitor.
- 5.4** There has been no use of RIPA since the last report in November 2014.
- 5.5** The Office of Surveillance Commissioners (OSC) oversees the use of covert surveillance by local authorities by carrying out three yearly inspections. The Council's most recent inspection took place 4 November 2015.
- 5.6** Refresher training was held 30 September 2015 for both the Senior Responsible Officer and the three Authorising Officers. The policy at Appendix One reflects some minor updates which are highlighted for members' attention via the use of 'track changes'.

<b>IMPLICATIONS</b>	
Finance	There are no direct financial implications associated with the changes. Training for staff, to ensure that they are kept up to date with good enforcement practices and revisions to RIPA, will be met from existing budgets.
Legal	The approval of the recommendation will ensure that the statutory requirements have been complied with.

**OTHER RISKS/IMPLICATIONS: CHECKLIST**

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

<b>Implications</b>	<b>✓ / x</b>
Community Safety	x
Equality and Diversity	x
Sustainability	x
Health and Safety	x

<b>Risks/Implications</b>	<b>✓ / x</b>
Asset Management	x
Climate Change	x
Data Protection	x

Report Author	Telephone No.	Email	Date
Philippa Davies	01253 887370	<a href="mailto:philippa.davies@wyre.gov.uk">philippa.davies@wyre.gov.uk</a>	29.09.15

<b>List of Background Papers:</b>		
Name of Document	Date	Where available for inspection

**LIST OF APPENDICES**

Appendix 1 – Updated RIPA Policy

arm/audit/cr/15/1011pd3



# Wyre Borough Council

## Policy Statement

### **The Regulation of Investigatory Powers Act, 2000 (RIPA)**

November 2015<sup>4</sup>

# Contents

Chapter		Page
1.	Introduction	1
2.	Directed Surveillance	2- <del>45</del>
3.	Covert Use of Human Intelligence Source (CHIS)	<del>45-67</del>
4.	Duration, Authorisation, Reviews, Renewals and Cancellations	7-13
5.	Communications Data	13-14
6.	Other Factors to Consider	15-17
7	Central Register	17
8.	Codes of Practice	17 <del>8</del>
9.	Benefits of Obtaining Authorisations under RIPA <del>S</del>	18
10.	Scrutiny and Tribunal	18 <del>9</del>
11.	Covert Surveillance of Social Networking Sites(SNS)	19-20
12.	Conclusion	20
	Appendix 1 - Definitions	21-22
	Appendix 2 - Scheme of Delegation	23- <del>24</del>
	Appendix 3 - Examples	<del>24-25-26</del>
	Appendix 4 - Codes of Practice 201 <del>4</del> 0	<a href="http://www.homeoffice.gov.uk">www.homeoffice.gov.uk</a>
	Appendix 5 -RIPA 2000	<a href="http://www.homeoffice.gov.uk">www.homeoffice.gov.uk</a>

Appendix 6 OSC Procedures and Guidance

*surveillancecom  
missioners.indep  
endent.gov.uk*

Appendix 7 - s.37 and 38 of the Protection of  
Freedoms Act 2012 and RIPA (Directed Surveillance  
and Covert Human Intelligence Sources)  
(Amendment) Order 2012.

[www.legislation.  
gov.uk](http://www.legislation.gov.uk)

Appendix 8 – Home Office Guidance Protection of  
Freedoms Act 2012.

[www.homeoffice.  
gov.uk](http://www.homeoffice.gov.uk)

Appendix 9 – RIPA Forms

intranet - RIPA

[Appendix 10- RIPA Directed Surveillance Decision  
Chart for Local authorities](#)

27

## 1. Introduction

- 1.1 **The Regulation of Investigatory Powers Act 2000 (RIPA)** regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.
- 1.2 Wyre Borough Council is therefore included within the RIPA framework with regard to the **authorisation of both Directed Surveillance** and of the use of **Covert Human Intelligence Sources** and access to **Communications Data**.
- 1.3 The purpose of this guidance is to:-
- explain the scope of RIPA and the circumstances where it applies
  - provide guidance on the authorisation procedures to be followed.
- 1.4 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and copies are attached at Appendix 4.
- 1.5 In summary, RIPA requires **that when the Council undertakes "directed surveillance" or uses a "covert human intelligence source"** these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. Following changes made by the Protection of Freedoms Act 2012 all authorisations must be approved by a magistrate from 1st November 2012. An extract from the Scheme of Delegation indicating the Authorising Officers is attached at Appendix 2.
- 1.6 Authorisation under RIPA gives lawful authority to carry out **directed surveillance** and the use of a **covert human intelligence source**. Obtaining authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention on Human Rights which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be "in accordance with the law". Provided activities undertaken are also "reasonable and proportionate" they will not be in contravention of Human Rights legislation.
- 1.7 Authorising Officers and investigators within the Local Authority are to note that RIPA does **not** extend powers to conduct **Intrusive Surveillance** (see para 2.4.5). Investigators should familiarise themselves with the provisions of the Code of Practice on Directed Surveillance and Covert Human Intelligence Sources (Appendix 4) to ensure a good understanding of the limitation of powers within RIPA.

- 1.8 Deciding when authorisation is required involves making a judgment. Paragraph 2.4 explains this process in detail. If you are in doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Senior Solicitor.

## 2. Directed Surveillance

### 2.1 What is meant by Surveillance?

#### “Surveillance” includes:-

- a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
- b) recording anything monitored, observed or listened to in the course of surveillance; and
- c) surveillance by or with the assistance of a surveillance device.

### 2.2 When is surveillance directed?

Surveillance is ‘**Directed**’ for the purposes of RIPA if it is **covert**, but **not intrusive** and is undertaken:

- a) for the purposes of a specific investigation or a specific operation.
- b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
- c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

### 2.3 Surveillance becomes intrusive if the covert surveillance:

- a) is carried out in relation to anything taking place on any “residential premises” or in any “private vehicle”; and
- b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or
- c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

**It should be noted that the Council cannot authorise “intrusive surveillance”.**



**2.4** Before any officer of the Council undertakes **any surveillance** of any individual or individuals they need to assess whether the activity comes within RIPA. In order to do this the following **key questions** need to be asked.

**2.4.1** ***Is the surveillance covert?***

**Covert surveillance** is that carried out in a manner **calculated** to ensure that subjects of it are unaware it is or may be taking place.

If activities are **open** and not hidden from the subjects of an investigation, the RIPA framework **does not** apply.

Examples of surveillance are provided given in in the Revised Code of Practice 2014 and are summarised in Appendix 3.

**2.4.2** ***Is it for the purposes of a specific investigation or a specific operation?***

If Officers are monitoring general activity in a street or car park, whether covert or overt, then it is not covered by RIPA, as such general observation duties are part of the legislative functions of public authorities and are not pre-planned surveillance of a specific person or group of people.

**2.4.3** ***Is it in such a manner that is likely to result in the obtaining of private information about a person?***

**“Private information”** is any information relating to a person’s private or family life.

It is an issue of fact and degree, which has to be examined in each case.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person’s activities may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person’s activities for future consideration.

Example: Officers of a local authority wish to drive past a café for purpose of taking a photograph of the exterior. This is not likely to require a directed surveillance authorisation, as no private information about any person is likely to be obtained. However if the authority, wish to establish a pattern of occupancy of the premises, the accumulation of information is likely to result in the obtaining of private information and a direct surveillance authorisation should be considered.

If it is likely that observations will not result in the obtaining of

private information about a person, then it is outside RIPA.

2.4.4 **Otherwise than by way of an immediate response to event or circumstances where it is not reasonably practicable to get authorisation**

The Home Office [Code of Practice 2014](#) gives the example of an immediate response to something happening during the course of an observer's work, which is unforeseeable e.g. a housing benefit fraud officer who conceals himself and continues to observe a person working who he knows to be claiming benefits and whom he comes across unexpectedly.

However, if as a result of that immediate response, a specific investigation subsequently takes place that brings it within the RIPA framework.

2.4.5 **Surveillance - Directed or Intrusive?**

**Directed surveillance** turns into **intrusive surveillance** if it is carried out involving anything that occurs on **residential** premises or any **private vehicle** and **involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.**

If the device is **not** on the premises or in the vehicle, it is **only intrusive surveillance** if it consistently **produces information of the same quality as if it were.**

**Commercial premises** and **commercial vehicles** are therefore **excluded** from intrusive surveillance.

High quality video monitoring or CCTV cameras may run a significant risk of providing consistently high quality data "as if you were there" and therefore come within the definition of intrusive surveillance.

Matron boxes ie. noise monitors, used by environmental health departments will not usually be covered. Usually they are stationed in a neighbouring property and do not provide evidence of the same quality as if the device was actually on the premises. Also the Code of Practice advises that in such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy.

The Council is **not** authorised to carry out **intrusive surveillance.**

**3. Covert use of Human Intelligence Source (CHIS)**

**3.1** A person is a **Covert Human Intelligence Source** if:

- a) he establishes or maintains a personal or other relationship with

a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c).

- b) he covertly uses such a relationship to obtain information or provide access to any information to another person; or
- c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

**3.2** A purpose is covert, in relation to the **establishment or maintenance** of a personal or other relationship, **if and only if** the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

**3.3** **A relationship** is used **covertly** and information obtained is disclosed **covertly, if and only if** it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

**3.4** An example given by the Home office is where intelligence suggests a local shopkeeper is selling alcohol to underage customers and the local authority engages an employee to act as a juvenile in order to make a purchase of alcohol. **In these circumstances any relationship, if established at all, is likely to be so limited, that the authority can conclude that an authorisation is unnecessary.**

### **3.5** Lay Witnesses

Choose carefully how you ask lay witnesses to gather information for you. For example, if a member of the public telephones to complain about noise nuisance caused by a neighbour. The third party is in a relationship with that person already and is just passing on information to the Council and would not be covered by RIPA. However the more the Council tasks a lay witness to do something then you may inadvertently change them into a CHIS.

If you are in any doubt seek advice from an Authorising Officer, and if they are in doubt they will seek advice from the Senior Solicitor.

### **3.6** The Use of Covert Human Intelligence Sources

3.6.1 In practice, it is most unlikely that it will ever be appropriate for the Council to utilise a CHIS. However, in the event that it is ever considered, advice should be sought from the Senior Solicitor at an early stage. It is potentially possible, that the role of a Council employee may be that of a source, or the Council may also use an external or professional source for the purpose of obtaining information. Such persons may be a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within

paragraphs b or c of paragraph 3.1.

- 3.6.2 Nothing in RIPA prevents material obtained by an employee acting as a source being used as evidence in Court proceedings.
- 3.6.3 The Authorising Officer must consider the safety and welfare of a CHIS acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given and considering what issues could be facing the security and welfare of a CHIS in relation to what they are to be asked to do. This should take place before any authorisation is granted, at any renewal, review and cancellation.
- 3.6.4 Before authorising the use of a CHIS as a source, the Authorising Officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.
- 3.6.5 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, “confidential material” is likely to be obtained (see definition of confidential material in Appendix 1). Special provisions relate to vulnerable individuals and juvenile services.
- 3.6.6 In addition to the usual authorisation process, the following management arrangements must be in place at all times in relation to the use of a CHIS:
1. there will be an appropriate officer of the Council ( ‘handler’) who has day-to-day responsibility for dealing with the CHIS, and for the security and welfare of the CHIS; and
  2. there will be a second appropriate officer of the Council who has general oversight of the use made of the CHIS, and who will have responsibility for maintaining an accurate and proper record about the source and tasks undertaken.(‘manager’ and ‘recorder’)
- 3.6.7 The CHIS forms contain appropriate boxes and prompts for ensuring the above is carried out.

## 4. Duration, Authorisations, Reviews, Renewals and Cancellations

### 4.1 Duration

#### 4.1.1 Authorisations lapse, if not renewed

- 4.1.1.1 **within 12 months** –from date of last renewal if it is for the conduct or use of a **covert human intelligence source** or
- 4.1.1.2 in all other cases (i.e. directed surveillance) **3 months** from the date of their grant or latest renewal.

#### 4.1.2 Directed Surveillance - Authorisation

4.1.2.1 For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

- a) that an authorisation is **necessary** (on the one the ground detailed below) and
- b) the authorised surveillance is **proportionate** to what is sought to be achieved by carrying it out.

4.1.2.2 An authorisation is **necessary** on the grounds stated below following the introduction of the Protection of Freedoms Act 2012:-

- a) for the purpose of preventing or detecting conduct which constitutes/corresponds to a criminal offence that is punishable by a maximum custodial sentence of 6 months or more or ~~constitutes an offence~~
- b) constitutes an offence under s.146, 147, or 147A of the Licensing Act 2003- selling alcohol to children or
- c) selling tobacco to persons under 18 years of age (s.7 Children and Young Persons Act 1933)

4.1.2.3 The Authorising Officer should set out, in his own words, why he believes the activity is necessary and proportionate. A bare assertion is insufficient. The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

- a) **necessary for the ground stated above and be able to demonstrate the reasons why it is necessary and;**
- b) **proportionate to its aim**

This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary.

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 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;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is important therefore that all officers involved in surveillance are fully aware of the extent and limits of the authorisation.

The Code of Practice 2014<sup>40</sup> gives an example of an individual suspected of carrying out a series of criminal damage offences at a local shop, after a dispute with the owner. It is suggested that a period of directed surveillance should be conducted against him to record his movements and activities for the purposes of preventing or detecting crime. Although these are legitimate grounds on which directed surveillance may be conducted, the Home Office code states that it is unlikely the interference with privacy will be proportionate in the circumstances of the particular case. In particular, the obtaining of private information

~~on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed, minor offence such as permitting dog fouling in a public place without clearing up afterwards. Although directed surveillance authorisation could be conducted, it advises that strong consideration should be given to the question of proportionality in the circumstances and suggests that general observation of the location may be undertaken instead, which would be less intrusive.~~

- 4.1.2.4 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained. ~~The applicant in completing the As such the forms provided must provide be completed facts and evidence where relevant.~~

It is also sensible to make any authorisation sufficiently wide enough to cover the means required as well as being able to prove effective monitoring of what is done against what is authorised.

- 4.1.2.5 Authorisations **must** be in ~~writing. The writing.~~ The standard forms to be used can be accessed via the Council's intranet.

- 4.1.2.6 IMPORTANT NOTE: THE PROTECTION OF FREEDOMS ACT 2012 INTRODUCES A REQUIREMENT FOR MAGISTRATE APPROVAL FOR ALL RIPA AUTHORISATIONS FROM 1st NOVEMBER 2012. ACCORDINGLY AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A JP HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E. A GRANT OR RENEWAL. The procedure and application process is set out in Annex A, B and C of Appendix 8. It is important that you seek advice from the Senior Solicitor before making the application for judicial approval.

- 4.1.2.7 Any Authorising Officer proposing to approve an application for the use of directed surveillance or for the use of a covert human intelligence source must immediately inform the Senior Solicitor who will then make arrangements for an application to be made to the Magistrates' Court.

- 4.1.2.8 **In such circumstances**, the Council will be required to

make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if and only if, at the date of the grant of authorisation or renewal of an existing authorisation they are satisfied that:

- (a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain.
- (b) the "relevant conditions" were satisfied in relation to the authorisation.

Relevant conditions include that:

- (i) the relevant person was designated as an Authorising Officer.
- (ii) it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with.
- (iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA (restrictions on the rank of the person granting the authorisation).
- (iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant or renewal of the authorisation, it may make an order to quash that authorisation. However the Court must not exercise its power to quash the authorisation unless the Council has had at least two business days from the date of the refusal in which to make representations.

#### 4.1.3 **Reviews**

- 4.1.3.1 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.
- 4.1.3.2 It is recommended that regular reviews be undertaken to see if the need for the surveillance is still continuing.



Results of reviews should be recorded in the Central Register of Authorisations (see paragraph 7). Reviews should be more frequent when access to confidential information or collateral intrusion is involved. Review frequency should be as often as the Authorising Officer deems necessary or practicable.

4.1.3.3 Each Authorising Officer will therefore determine in each case how often authorisations should be reviewed. It is recommended that they ensure records of the review be supplied on the relevant form. Copies should be sent to the Senior Solicitor to keep the Central Register up to date.

#### 4.1.4 **Renewals**

4.1.4.1 An Authorising Officer may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was given. A renewal of the authorisation in writing can be made for **3 months**. Applications for renewal should detail how many times an authorisation has been renewed; significant changes to the original application for authority; reasons why it is necessary to renew; content and value of the information obtained so far and results of regular reviews of the investigation or operation.

4.1.4.2 Each application to renew should be made at least **7 days** before the authorisation is due to expire on the relevant form. A record of the renewal should be kept within the applying service and supplied centrally to the Senior Solicitor to be placed in the Central Register.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 RENEWALS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE RENEWAL. SEE PARAGRAPH 4.1.2.6 - 4.1.2.8 ABOVE.

#### 4.1.5 **Cancellations**

4.1.5.1 All authorisations, including renewals should be cancelled if the need for the surveillance is no longer justified. This will occur in most cases where the purpose for which the surveillance was required has been achieved.

4.1.5.2 Requesting officers should ensure they inform Authorising Officers if this is the case before the next review. If, in the opinion of the Authorising Officer at the next review, the need for surveillance is no longer justified, it must be cancelled.

4.1.5.3 The cancellation forms will be used to record a cancellation; ~~the original will be kept with the service,~~ and the Authorising Officer will ensure the original cancellation has been sent to the Senior Solicitor or nominated representative to update the Central Register.

## **4.2 Covert Use of Human Intelligence Sources**

### **4.2.1 Authorisation**

4.2.1.1 The same principles as set out in paragraphs 4.1.2.1 and 4.1.2.2 apply to CHIS except the ground on which a CHIS can be authorised, which remains unaltered by the Protection of Freedoms Act 2012.

A CHIS authorisation can only be approved where it is necessary for the purpose of preventing or detecting crime, or of preventing disorder.

A CHIS authorisation can last for up to 12 months.

4.2.1.2 The conduct so authorised is any conduct that:

- a) is comprised in any such activities involving the conduct or use of a covert human intelligence source, as are specified or described in the authorisation;
- b) relates to the person who is specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and
- c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

4.2.1.3 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against what is authorised.

### **4.2.2 Renewals/Reviews**

4.2.2.1 Similar provisions apply for a CHIS except that a renewal here can last for a further 12 months, a review

must have been carried out on the use of the source and an application should only be made to renew when the initial authorisation period is drawing to an end. Applications to renew a CHIS also should contain use made of the source and tasks given to the source during the previous authorised period and the information obtained.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E. A GRANT OR RENEWAL. SEE PARAGRAPH 4.1.2.6-4.1.2.8 ABOVE.

#### 4.2.3 **Cancellations**

4.2.3.1 The same principles as Directed Surveillance apply.

4.2.3.2 Separate forms have been devised for applications to authorise, review, renew and cancel a CHIS. These can be accessed via the Council's intranet.

## 5. **Communications Data**

### 5.1 **Communications Data Order 201003**

The Regulation of Investigatory Powers (Communications Data) Order 2010 replaced the earlier 2003 order which gave 03 extends to local authorities the powers set out within RIPA to access communications data. The 2010 Order raised the seniority of the Authorising Officers in local authorities to a 'Director, Head of Service, Manager or equivalent.' Communications data includes information relating to the use of a communications service but does not include the contents of the communications itself. Communications data can be split into three types; "traffic data" i.e. where a communication was made from, to whom and when; "service data" is the use made of the service by any person eg itemised telephone records; and "subscriber data" i.e. any other information that is held or obtained by an operator on a person they provide a service to. Local authorities are allowed to access "service data" and "subscriber data"; they are not allowed to access "traffic data".

NOTE: An Investigatory Powers Bill was announced in the Queen's Speech in May 2015 relating to communications data. The bill's progress will be monitored and amendments to this policy will be made as and when required. The Communications Data Bill was published in draft form on 14th June 2012. The draft bill proposes to take communications data outside of the RIPA framework and create a new framework dealing with communications data. However, following the critical report of the Joint Committee on the bill in December 2012, the Home office confirmed the bill will now be redrafted. The government announced in the Queen's Speech in 2013 that it intends to bring forward proposals on the

~~investigation of crime in cyberspace. Although the speech does not include specific plans for a revival of the draft bill, it certainly contains nothing that would prevent the government from doing so either. Any changes to legislation will be kept under review and amendments to this policy will be made as required.~~

## **5.2 Authorisation**

The Order permits access to communications data, by local authorities only where it is necessary **for the purpose of preventing or of detecting** crime or preventing disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve. It should not be authorised where less intrusive means can be used to further an investigation

## **5.3 Alternative methods for authorisation**

Access to communications data may be authorised in two ways; either (a) through an authorisation by an Authorising Officer which would allow the authority to collect or retrieve data itself, or (b) by a notice given to a postal or telecommunications operator requiring that operator to collect or retrieve the data and provide it to the local authority.

## **5.4 Application**

Application will be made by the investigating officer and submitted to a Single Point of Ccontact (SPOC) who will either accept or reject the application. If the SPOC accepts the application he will forward it together with a SPOC report and a draft notice (where appropriate) to an Authorising Officer for authorisation.

If the Authorising officer accepts the application, it will need to be approved by a magistrate before the forms are returned to the SPOC and the SPOC will deal with the postal or telecommunications operator directly. The SPOC will also advise investigating officers and Authorising officers on whether an authorisation or a notice is appropriate in the circumstances.

Although it is unlikely that the Council will access communications data, in the event that it did, the Council would appoint a nominated SPOC from NAFN, (National Anti- Fraud Network), who have received training on a course recognised by the Home Office.

### **Authorising Officers**

Authorising Officers for the purposes of communications data will be the same as for directed surveillance and CHIS's.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION. SEE PARAGRAPHS 4.1.2.6 - 4.1.2.8 ABOVE.

## 6. **Other Factors to Consider**

6.1 Particular consideration should be given to **collateral intrusion** i.e. the risk of intrusion into the privacy of those not directly the targets of the investigation. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests, as outlined above, apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

6.2 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the surveillance.

6.3 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subject of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

6.4 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

### 6.5 **Confidential Material**

RIPA does not provide any special protection for '**confidential material**' (see the definitions in Appendix 1). Nevertheless, such material is particularly sensitive, and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation, i.e. by the chief Executive.

6.6 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

**6.7** The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be alerted to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Senior Solicitor before further dissemination takes place;
- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Senior Solicitor) is satisfied that it is necessary for a specific purpose;
- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.
- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

**6.8** In the case of **confidential information a higher level of authorisation** is required. Therefore where authorisation is sought to carry out surveillance in respect of communications subject to legal professional privilege, or containing confidential personal information or confidential journalistic material, the Chief Executive must sign their authorisation.

**6.9** **Joint Working**

In cases of joint working, where one agency is acting on behalf of another, usually the tasking agency can obtain or provide the authorisation i.e. if the Council has been tasked by the Police to assist in a covert surveillance operation, they should get the authorisation, which would then cover the Council. But advice should be sought from the Senior Solicitor prior to any arrangements being agreed.

**6.10** **Handling and Disclosure of Materials**

Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 6.7 above.

**6.11** Applications and associated reviews, renewals and cancellations for directed surveillance shall be centrally retrievable for a period of 53 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

**6.12** Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation

or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer. If in doubt advice should be sought from the Senior Solicitor.

**6.13** There is nothing in RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the Council, of any material obtained by means of covert surveillance and, other than in pursuance of the ground, on which it was obtained, should be authorised only in the most exceptional circumstances. Advice should be sought from the Senior Solicitor.

## **7. Central Register of Authorisation**

**7.1** The RIPA Code of Practice requires a central register of all authorisations to be maintained. **The Legal Section maintains this register.**

**7.2** Whenever an authorisation is authorised, renewed, reviewed or cancelled the Authorising Officer must send the signed original authorisation to the Senior Solicitor or nominated representative. Receipt of the form will be acknowledged.

**7.3** The Central Register will contain the following information:

- the type and date of authorisation
- the name and grade of the Authorising Officer
- a unique reference number for the investigation or operation
- the title of the investigation/operation, and a brief description and names of the subjects, if known
- ~~if the urgency provisions were used, and why~~
- if an authorisation is renewed, when and the name and designation of the Authorising Officer
- if confidential information is likely to be a consequence of the investigation or operation
- the date the authorisation was cancelled.  
the date of magistrates court approval

**7.4** The legal section will securely retain the original authorisations and maintain the Central Register. Authorisations should only be kept for a minimum of 53 years from the end of an authorisation. Once the investigation is closed (bearing in mind cases may be lodged some time after the initial work) the records held by the department should be disposed of in an appropriate manner (e.g. shredded).

## **8. Codes of Practice**

There are Home Office codes of practice and Office of Surveillance Commissioners (OSC) Guidance that expand on this policy guidance and statement and copies are attached at Appendices ~~ces~~ 4 and 6. The Codes

also lists General Best Practices, which should be followed where at all possible.

The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, “if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account”.

**Staff should refer and familiarise themselves with the Home Office Codes of Practice-Practice and OSC Guidance for supplementary guidance.**

**Authorising Officers and the Senior Responsible Officer (Senior Solicitor) should also familiarise themselves with the Procedures and Guidance document produced by the OSC attached at Appendix 6.**

## **9. Benefits of Obtaining Authorisation Under RIPA**

### **9.1 Authorisation of surveillance and human intelligence sources**

RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and
- the conduct is in accordance with the authorisation, then
- it shall be “lawful for all purposes”.

However, the corollary is not true – i.e. if you do not obtain RIPA authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits.

### **9.2 RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which –**

- a) is incidental to any conduct that is lawful by virtue of an authorisation; and
- b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

## **10 Scrutiny and Tribunal**

**10.1** The Surveillance Commissioner will regulate conduct carried out under RIPA. The Surveillance Commissioner and his assistants to ensure RIPA compliance are conducting a programme of inspection of Local Authorities.



**10.2** RIPA provides for the establishment of a tribunal to consider and determine complaints made under RIPA, and persons aggrieved by a local authority's conduct e.g. directed surveillance can make complaints to the tribunal. The forum hears applications on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among other things, the quashing or cancellation of any authorisation and can order destruction of any records or information obtained by such authorisation, and records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

- A Council Officer has granted any authorisation under RIPA.
- Council employees have engaged in any/all conduct as a result of such authorisation.
- A disclosure notice requirement is given.

## **11 Covert Surveillance of Social Networking Sites (SNS)**

**11.1** The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

**11.2** Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though 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. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

**11.3** If it is necessary and proportionate for a public authority to breach covertly 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 a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content). This could occur if an officer asks to become a 'friend' of someone on a social networking site.

**11.4** It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes

other laws.

- 11.5** A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done.

## **12 Conclusion**

- 12.1** If you can carry out investigations in an obviously overt way so that it does not compromise what you are trying to achieve then that is the best way. However, if you need to do things covertly, then you need to consider RIPA and you are advised to take a wide view and interpretation of your activities. If you are in doubt you can seek advice from Senior Solicitor and remember if there is any doubt then it is usually safer to get an authorisation.

**Definitions from the 2000 Act**

- **“RIPA”** means the Regulation of Investigatory Powers Act 2000.
- **“Confidential Material”** consists of:
  - a) matters subject to legal privilege;
  - b) confidential personal information; or
  - c) confidential journalistic material
- **“Matters subject to legal privilege”** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below)
- **“Confidential Personal Information”** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:
  - a) to his/her physical or mental health; or
  - b) to spiritual counselling or other assistance given or to be given, and  

which a person has acquired or created in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office (See Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:
  - c) it is held subject to an express or implied undertaking to hold it in confidence; or
  - d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.
- **“Confidential Journalistic Material”** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.
- **“Covert Surveillance”** means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;
- **“Authorising Officer”** means a person designated for the purposes of RIPA to grant authorisations for directed surveillance.

**Note A** *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.*

**Note B** *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

## **Extract from Part 7 of the Council's Constitution- Management Structure and Scheme of Delegation**

### **Scheme of Delegation to Officers – General**

All delegations to officers are subject to the following general conditions:

( 2) In the absence of the Chief Executive the functions of the Chief Executive will be the responsibility of either of the Corporate Directors

### **Executive Functions Delegated to the Chief Executive**

(7) To provide the necessary authorisations in respect of surveillance in accordance with the Regulation of Investigatory Powers Act 2000, where confidential information is involved or where authorisation is sought for the employment of a juvenile or vulnerable Covert Human Intelligence Source (CHIS).

~~In the absence of the Chief Executive the functions of the Chief Executive will be the responsibility of either of the Corporate Directors.~~

### **Scheme of Delegation – Authority Given to the Chief Executive (Head of Paid Service) – Garry Payne**

~~(9) To provide the necessary authorisations in respect of surveillance in accordance with the Regulation of Investigatory Powers Act 2000, where confidential information is involved or where authorisation is sought for the employment of a juvenile or vulnerable CHIS.~~

### **Executive Functions Delegated to the Corporate Directors**

#### **Scheme of Delegation – Authority Given to the Chief Executive and Corporate Directors – Philippa Davies and Michael Ryan**

~~(27) To act as authorising officers for the purposes of the Regulation of Investigatory Powers Act 2000 and Protection of Freedoms Act 2012.~~

### **Executive Functions Delegated to the Senior Solicitor**

(3) To act as the Senior Responsible Officer for the purpose of Part II of the Regulation of Investigatory Powers Act 2000

(4) To make an application to a Justice of the Peace in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the Council in making such an application.

### **Executive Functions Delegated to Fraud and Compliance Manager and Fraud Investigation Officers**

(1) To make an application to a Justice of the Peace, in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the Council in making such an application

(3)Power to carry out surveillance which is governed by the Regulation of Investigatory Powers Act 2000 as agreed by an authorising officer.

Examples of Surveillance

Examples of different types of Surveillance.	Examples
Surveillance that does <u>not</u> require RIPA Authorisation	<ul style="list-style-type: none"> <li>- Council officers on patrol, who conceal themselves to observe suspicious persons that they come across in the course of a routine patrol.</li> <li>- Signposted Town Centre CCTV cameras (in normal use)</li> <li>- Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.</li> <li>- Sampling purchases (where the officer behaves no differently from a normal member of the public).</li> <li>- Dog Warden in uniform on patrol in park, street or van</li> <li>- Food Safety or Health &amp; Safety Inspections</li> <li>- <del>General observational duties not specifically targeted/planned or considered directed surveillance. Plain clothes officers on patrol to monitor a crime hot spot. Their objective is to observe a location and is a general observational activity rather than surveillance of individuals and the obtaining of private information is unlikely.</del></li> <li>- CCTV cameras providing general traffic, crime or public safety information</li> <li>- Covert surveillance of an employee who is suspected by his employer of undertaking additional duties in breach of discipline regulations, as it does not relate to the discharge of the Employer's core functions.</li> </ul>
Covert Directed Surveillance must be RIPA authorised.	Officers follow/observe an individual or individuals over a period, to establish whether s/he is working when claiming benefit provided the conduct constitutes/corresponds to a criminal offence punishable with at least 6 months imprisonment
Surveillance that is not intrusive	- An observation post outside residential premises, which provides a limited view compared to that which would be achievable from within the premises.

Intrusive – **Council cannot do this!**

- Planting a listening or other device in a person's home or in their private vehicle.
- Use of a zoom lens outside residential premises, which consistently achieves imagery of the same quality as that which would be visible from within the premises.





*cutting through complexity*

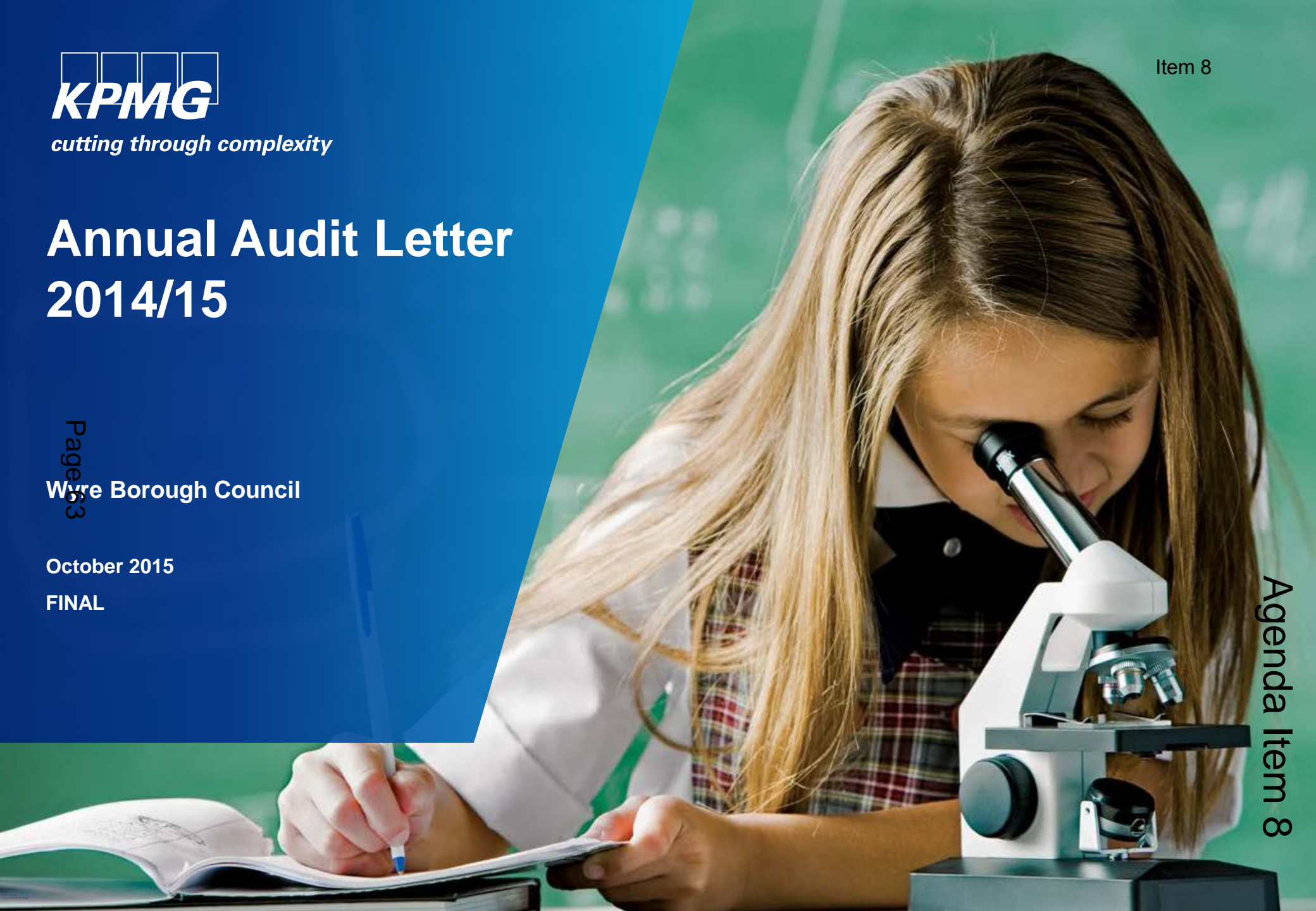
# Annual Audit Letter 2014/15

Pages  
33  
Wyre Borough Council

October 2015

FINAL

Item 8



Agenda Item 8

The contacts at KPMG in connection with this report are:

**Tim Cutler**

Partner  
KPMG LLP (UK)

Tel: 0161 246 4774  
[tim.cutler@kpmg.co.uk](mailto:tim.cutler@kpmg.co.uk)

**Jillian Burrows**

Senior Manager  
KPMG LLP (UK)

Tel: 0161 246 4705  
[jillian.burrows@kpmg.co.uk](mailto:jillian.burrows@kpmg.co.uk)

**Chris Paisley**

Manager  
KPMG LLP (UK)

Tel: 0161 246 4394  
[christopher.paisley@kpmg.co.uk](mailto:christopher.paisley@kpmg.co.uk)

**Report sections**

- Headlines

**Appendices**

1. Summary of reports issued
2. Audit fees

**Page**

2

4

5

This report is addressed to the Authority and has been prepared for the sole use of the Authority. We take no responsibility to any member of staff acting in their individual capacities, or to third parties. The Audit Commission issued a document entitled *Statement of Responsibilities of Auditors and Audited Bodies* summarising where the responsibilities of auditors begin and end and what is expected from audited bodies. We draw your attention to this document which is available on Public Sector Audit Appointment's website ([www.psa.co.uk](http://www.psa.co.uk)).

External auditors do not act as a substitute for the audited body's own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

We are committed to providing you with a high quality service. If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Tim Cutler, the engagement lead to the Authority, who will try to resolve your complaint. If you are dissatisfied with your response please contact the national lead partner for all of KPMG's work under our contract with Public Sector Audit Appointments Limited, Trevor Rees (on 0161 246 4000, or by email to [trevor.rees@kpmg.co.uk](mailto:trevor.rees@kpmg.co.uk)). After this, if you are still dissatisfied with how your complaint has been handled you can access PSA's complaints procedure by emailing [generalenquiries@psaa.co.uk](mailto:generalenquiries@psaa.co.uk), by telephoning 020 7072 7445 or by writing to Public Sector Audit Appointments Limited, 3rd Floor, Local Government House, Smith Square, London, SW1P 3HZ.

This report summarises the key findings from our 2014/15 audit of Wyre Borough Council (the Authority).

Although this letter is addressed to the Members of the Authority, it is also intended to communicate these issues to key external stakeholders, including members of the public.

Our audit covers the audit of the Authority's 2014/15 financial statements and the 2014/15 VFM conclusion.

<p><b>VFM conclusion</b></p>	<p>We issued an unqualified conclusion on the Authority's arrangements to secure value for money (VFM conclusion) for 2014/15 on 29 September 2015. This means we are satisfied that that Authority had proper arrangements for securing financial resilience and challenging how it secures economy, efficiency and effectiveness.</p> <p>To arrive at our conclusion we looked at the Authority's financial governance, financial planning and financial control processes, as well as the arrangements for prioritising resources and improving efficiency and productivity.</p> <p>We undertook a risk assessment as part of our VFM audit work to identify the key areas impacting on our VFM conclusion and considered the arrangements you have put in place to mitigate these risks.</p> <p>We did not identify any specific risks during these risk assessment processes which would impact on our VFM conclusion for 2014/15.</p>
<p><b>Audit opinion</b></p>	<p>We issued an unqualified opinion on the Authority's financial statements on 29 September 2015. This means that we believe the financial statements give a true and fair view of the financial position of the Authority and of its expenditure and income for the year.</p>
<p><b>Financial statements audit</b></p>	<p>We did not identify any material misstatements as a result of our audit work. We did, however, agree with management a small number of presentational adjustments to the accounts during the course of our audit.</p> <p>We identified one audit issue in 2014/15 which has been communicated to management. This resulted in a low priority recommendation within our report to those charged with governance, as follows:</p> <ul style="list-style-type: none"> <li>■ Monthly payroll 'starting figure' reconciliations should be signed as prepared and reviewed when completed. These reconciliations compare the monthly payroll data for each individual member of staff with the amount paid in the previous month, providing assurance over the changes made to payroll data in the intervening period.</li> </ul>
<p><b>Annual Governance Statement</b></p>	<p>We reviewed your <i>Annual Governance Statement</i> and concluded that it was consistent with our understanding.</p>

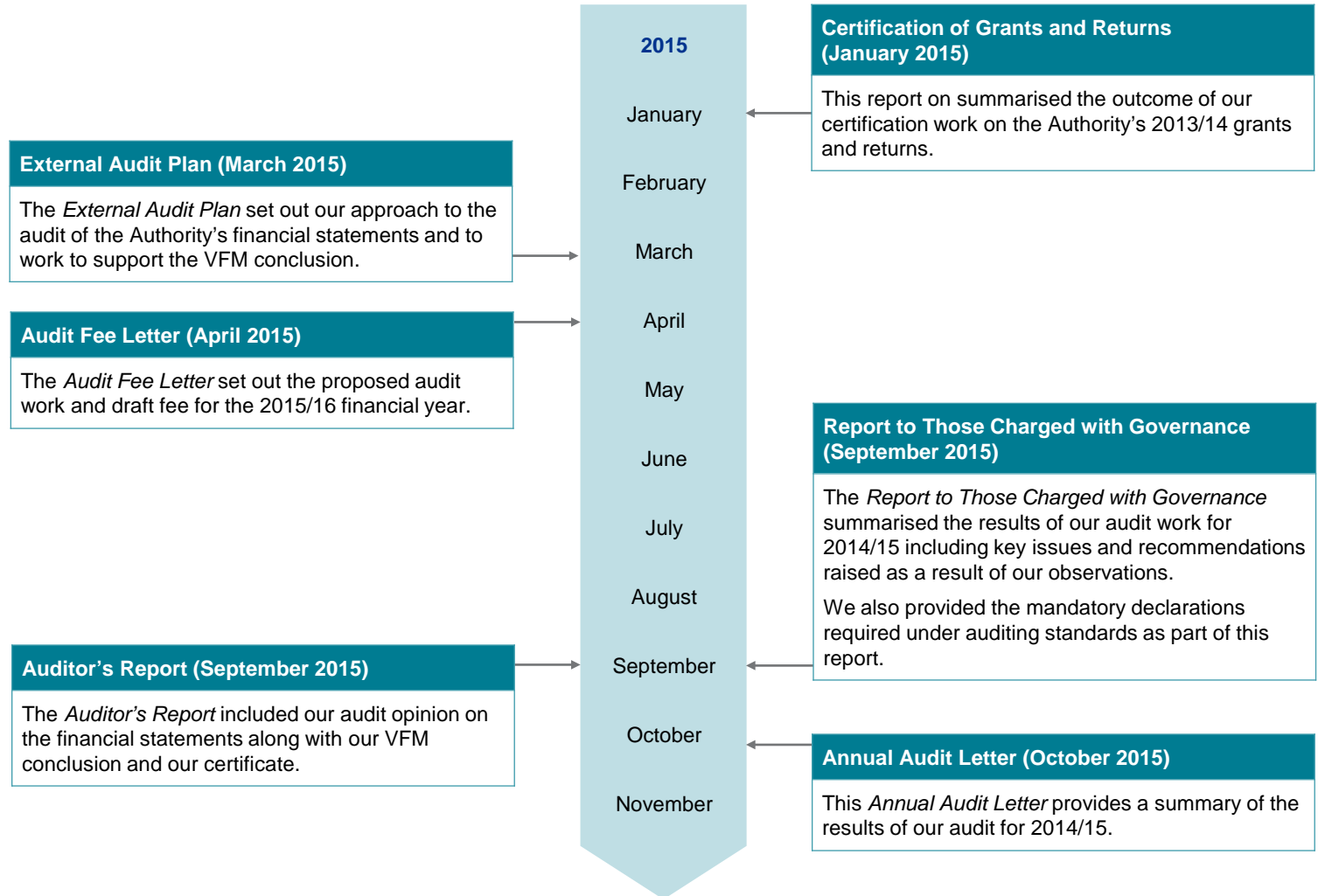
All the issues in this Annual Audit Letter have been previously reported. The detailed findings are contained in the reports we have listed in Appendix 1.

<b>Whole of Government Accounts</b>	<p>The Authority prepares a consolidation pack to support the production of Whole of Government Accounts by HM Treasury. We are not required to review your pack in detail as the Authority falls below the threshold where an audit is required. As required by the guidance we have confirmed this with the National Audit Office.</p>
<b>High priority recommendations</b>	<p>We raised no high priority recommendations as a result of our 2014/15 audit work. The low priority recommendation we made has been outlined on page 2 of this report.</p>
<b>Certificate</b>	<p>We issued our certificate on 29 September 2015. The certificate confirms that we have concluded the audit for 2014/15 in accordance with the requirements of the <i>Audit Commission Act 1998</i> and the Audit Commission's <i>Code of Audit Practice</i>.</p>
<b>Audit fee</b>	<p>Our fee for 2014/15 was £64,883, excluding fees for certification of grants claims and VAT. This is in line with the planned fee for 2014/15, and the fee for the 2013/14 audit.</p> <p>Our 2014/15 fee is an increase of £900 from the position set out in our Audit Fee Letter for 2014-15. The increase is due to additional work we were required to undertake on the collection fund balances, following the end of the requirement for us to certify the Authority's NNDR return</p> <p>Further detail is contained in Appendix 2.</p>

## Appendix 1: Summary of reports issued

This appendix summarises the reports we issued since our last *Annual Audit Letter*.

Page 67



**This appendix provides information on our final fees for the 2014/15 audit.**

To ensure transparency about the extent of our fee relationship with the Authority we have summarised below the outturn against the 2014/15 planned audit fee.

#### **External audit**

Our final fee for the 2014/15 audit of the Authority was £64,883, which is in line with the planned fee.

This is an increase of £900 from the position set out in our Audit Fee Letter for 2014-15, issue in May 2014. The increase is due to additional work we were required to undertake on the collection fund balances, following the end of the requirement for us to certify the Authority's NNDR return

Our fees are still subject to final determination by Public Sector Audit Appointments.

#### **Certification of grants and returns**

Under our terms of engagement with Public Sector Audit Appointments we undertake prescribed work in order to certify the Authority's housing benefit grant claim. This certification work is still ongoing. The final fee will be confirmed through our reporting on the outcome of that work in January 2016.



*cutting through complexity*

Page 69

© 2015 KPMG LLP, a UK public limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International Cooperative (KPMG International).

arm/audit/cr/15/1011pd2

This page is intentionally left blank





## Public Sector Audit Appointments

19 October 2015

**Subject: Consultation on the 2016/17 work programme and scales of fees**

Dear Ms Davies

Public Sector Audit Appointments Limited (PSAA) is responsible for managing the audit contracts previously let by the Audit Commission, and will set 2016/17 scale audit fees for relevant audited bodies under statutory powers delegated to it by the Secretary of State for Communities and Local Government.

PSAA is now consulting on the proposed work programme and scales of fees for 2016/17 audits. The consultation sets out the work that auditors will undertake at relevant principal audited bodies, with the associated scales of fees.

There are no planned changes to the overall work programme for 2016/17. We propose that scale fees are set at the same level as the scale fees applicable for 2015/16, set by the Audit Commission before it closed in March 2015. The Commission reduced scale fees from 2015/16 by 25 per cent, in addition to the reduction of up to 40 per cent made from 2012/13.

Following completion of the Audit Commission's 2014/15 accounts, PSAA has received a payment in respect of the Audit Commission's retained earnings. PSAA will redistribute this and any other surpluses from audit fees to audited bodies, on a timetable to be established shortly.

The work that auditors will carry out on the 2016/17 accounts will be completed based on the requirements set out in the Local Audit and Accountability Act 2014 and under the Code of Audit Practice published by the National Audit Office.

The consultation documents on the 2016/17 proposed work programme and scales of fees are now available for you to view on the PSAA website at <http://www.psaa.co.uk/audit-and-certification-fees/consultation-on-201617-proposed-fee-scales/>

We hope you find this information useful. We welcome comments on the consultation proposals, which should be sent to:

[workandfeesconsultation@psaa.co.uk](mailto:workandfeesconsultation@psaa.co.uk)

or by post to Jon Hayes, Chief Officer, at: Public Sector Audit Appointments Limited, 3rd Floor, Local Government House, Smith Square, London SW1P 3HZ.

The consultation will close on **Friday 15 January 2016**.

Yours sincerely

Jon Hayes  
Chief Officer

arm/audit/cr/15/1011pd1