



Borough of Tamworth

Marmion House,
Lichfield Street, Tamworth,
Staffordshire B79 7BZ.

Enquiries: 01827 709 709
Facsimile: 01827 709 271

AUDIT AND GOVERNANCE COMMITTEE

20 January 2016

Dear Councillor

A meeting of the Audit and Governance Committee will be held in **Committee Room 1 - Marmion House on Thursday, 28th January, 2016 at 6.00 pm**. Members of the Committee are requested to attend.

Yours faithfully

A handwritten signature in black ink, appearing to be 'A. D. ...', written over a circular stamp.

A G E N D A

NON CONFIDENTIAL

- 1 Apologies for Absence
- 2 Minutes of the Previous Meeting (Pages 1 - 4)
- 3 Declarations of Interest

To receive any declarations of Members' interests (pecuniary and non-pecuniary) in any matters which are to be considered at this meeting.

When Members are declaring a pecuniary or non-pecuniary interest in respect of which they have dispensation, they should specify the nature of such interest. Members should leave the room if they have a pecuniary or non-pecuniary interest in respect of which they do not have a dispensation.

- 4 Annual Audit Letter 2014/15** (Pages 5 - 10)
The Report of Grant Thornton (External Auditor)
- 5 Tamworth BC Audit and Governance Committee Update Paper** (Pages 11 - 28)
The Report of Grant Thornton (External Auditor)
- 6 Internal Audit Annual Report/Quarterly Report 2015/16 Quarter 3** (Pages 29 - 44)
(Report of the Head of Internal Audit Services)
- 7 Risk Management Update Report** (Pages 45 - 54)
(Report of the Head of Internal Audit Services)
- 8 Fraud & Corruption Update Report** (Pages 55 - 70)
(Report of the Head of Internal Audit Services)
- 9 Quarterly RIPA Report January 2016** (Pages 71 - 74)
(Report of the Solicitor to the Council and Monitoring Officer)
- 10 Updated RIPA Policy** (Pages 75 - 122)
(Report of the Solicitor to the Council)
- 11 Standards Allegation Complaint** (Pages 123 - 126)
(Report of the Solicitor to the Council)
- 12 Audit and Governance Committee Timetable** (Pages 127 - 130)
(Discussion Item)

People who have a disability and who would like to attend the meeting should contact Democratic Services on 01827 709264 or e-mail committees@tamworth.gov.uk preferably 24 hours prior to the meeting. We can then endeavour to ensure that any particular requirements you may have are catered for.

To Councillors: J Chesworth, J Oates, J Faulkner, J Goodall, S Goodall, K Norchi and
T People

This page is intentionally left blank



MINUTES OF A MEETING OF THE AUDIT AND GOVERNANCE COMMITTEE HELD ON 29th OCTOBER 2015

PRESENT: Councillor J Chesworth (Chair), Councillors J Faulkner, J Goodall, S Goodall, K Norchi and T People

Officers John Wheatley (Executive Director Corporate Services) and Angela Struthers (Head of Internal Audit Services)

35 APOLOGIES FOR ABSENCE

Apologies for absence were received from Councillor Jeremy Oates

36 MINUTES OF THE PREVIOUS MEETING

The minutes of the meeting held on 24 September 2015 were approved and signed as a correct record.

(Moved by Councillor K Norchi and seconded by Councillor S Goodall)

37 DECLARATIONS OF INTEREST

There were no declarations of Interest.

38 FRAUD AND CORRUPTION UPDATE REPORT

The Head of Internal Audit provided Members with an update of Counter Fraud work completed to date during the financial year 2015/16.

RESOLVED:

- That the Committee
- 1 endorsed the Checklist for those Responsible for Combating Fraud and Corruption (Appendix 1);
 - 2 approved the Counter Fraud and Corruption Policy Statement, Strategy and Guidance Notes (Appendix 2);
 - 3 approved the Whistleblowing Policy (Appendix 3);

and

- 4 endorsed the Fraud Risk Register Summary (Appendix 4)

(Moved by Councillor J Faulkner and seconded by Councillor S Goodall)

39 INTERNAL AUDIT QUARTERLY REPORT

The Head of Internal Audit Services reported on the outcome of Internal Audit's review of the internal control, risk management and governance framework in the 2nd Quarter of 2015/16 – and provided members with assurance of the ongoing effective operation of an internal audit function and to enable any particularly significant issues to be brought to the Committee's attention.

RESOLVED: That the Committee considered the Quarterly Report and had no issues to raise

(Moved by Councillor T Peaple and seconded by Councillor J Goodall)

40 RISK MANAGEMENT UPDATE 2015/16

The Head of Internal Audit reported on the Risk Management process and progress to date for the current financial year.

RESOLVED: That the Committee

- 1 approved the revised Risk Management Policy and Strategy;
- 2 endorsed the Corporate Risk Register; and
- 3 endorsed the Risk Management Action Plan

(Moved by Councillor J Faulkner and seconded by Councillor J Chesworth)

41 AUDIT AND GOVERNANCE COMMITTEE TIMETABLE

The Committee reviewed and agreed the timetable.

Chair

This page is intentionally left blank

The Annual Audit Letter for Tamworth Borough Council

Year ended 31 March 2015

October 2015

Page 5

John Gregory

Engagement Lead

T 0121 232 5333

E john.gregory@uk.gt.com

Joan Barnett

Manager

T 0121 232 5399

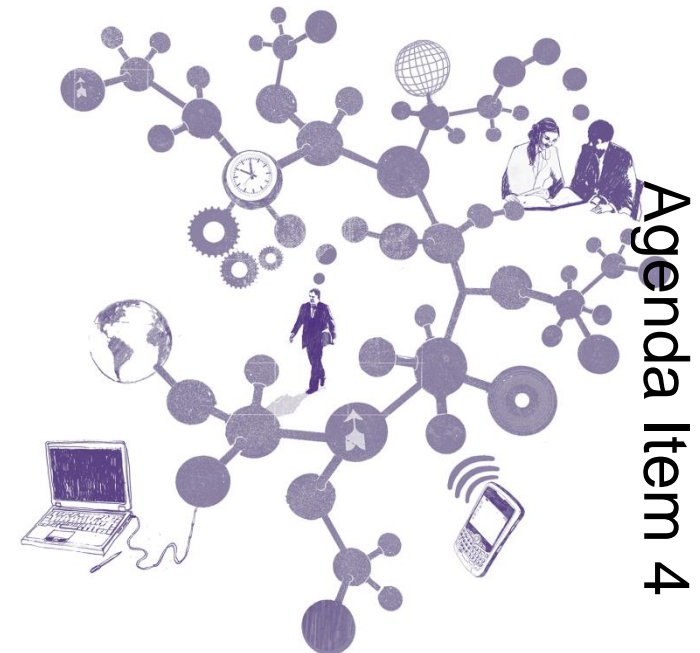
E joan.m.barnett@uk.gt.com

Denise Mills

In-Charge Auditor

T 0121 232 5306

E denise.f.mills@uk.gt.com



Agenda Item 4

Contents

Section	Page
1. Key messages	3
Appendices	
A Summary of reports and audit fees	5

Page 6

Key messages

Our Annual Audit Letter summarises the key findings arising from the work that we have carried out at Tamworth Borough Council ('the Council') for the year ended 31 March 2015.

The Letter is intended to communicate key messages to the Council and external stakeholders, including members of the public. Our annual work programme, which includes nationally prescribed and locally determined work, has been undertaken in accordance with the Audit Plan that we issued on 26 March 2015 and was conducted in accordance with the Audit Commission's Code of Audit Practice, International Standards on Auditing (UK and Ireland) and other guidance issued by the Audit Commission and Public Sector Audit Appointments Limited.

<p>Financial statements audit (including audit opinion)</p> <p>Page 7</p>	<p>We reported our findings arising from the audit of the financial statements in our Audit Findings Report on 24 September 2015 to the Audit and Governance Committee. The key messages reported were:</p> <ul style="list-style-type: none">• the Council's arrangements to prepare the financial statements ensured the draft accounts were of a good quality• the audit did not identify any audit adjustments that affected the Council's reported financial position• the audit did identify a small number of adjustments to improve the presentation of the financial statements. <p>We issued an unqualified opinion on the Council's 2014/15 financial statements on 24 September 2015, meeting the deadline set by the Department for Communities and Local Government. Our opinion confirms that the financial statements give a true and fair view of the Council's financial position and of the income and expenditure recorded by the Council.</p>
<p>Value for Money (VfM) conclusion</p>	<p>We issued an unqualified VfM conclusion for 2014/15 on 24 September 2015.</p> <p>On the basis of our work, and having regard to the guidance on the specified criteria published by the Audit Commission, we are satisfied that in all significant respects the Council put in place proper arrangements to secure economy, efficiency and effectiveness in its use of resources for the year ending 31 March 2015.</p>

Key messages continued

Certification of housing benefit grant claim	Our work on certification of grant claims is on-going. Our work to date has not identified any issues which we wish to highlight. The indicative fee for this work remains £15,530 and will be confirmed alongside the detailed findings of our work in our Grant Certification report, due for presentation to the Audit and Governance Committee upon completion of our work.
Audit fee	Our fee for 2014/15 was £65,550, excluding VAT which was in line with our planned fee for the year and represented a reduction of 1.4% from the previous year. Further detail is included within appendix A.

Appendix A: Reports issued and fees

We confirm below the fees charged for the audit and non-audit services.

Fees for audit services

	Per Audit plan £	Actual fees £
Council audit	65,550	65,550
Housing benefit grant certification fee	15,630	15,630
Total audit fees	81,180	81,180

Fees for other services

Service	Fees £
Non-audit related services	Nil

Reports issued

Report	Month issued
Audit Plan	March 2015
Audit Findings Report	September 2015
Annual Audit Letter	October 2015
Certification Report	December 2015 (planned)



© 2015 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton is a member firm of Grant Thornton International Ltd (Grant Thornton International). References to 'Grant Thornton' are to the brand under which the Grant Thornton member firms operate and refer to one or more member firms, as the context requires. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by member firms, which are not responsible for the services or activities of one another. Grant Thornton International does not provide services to clients.

grant-thornton.co.uk

Tamworth Borough Council Audit and Governance Committee Update 28 January 2016

Year ended 31 March 2016

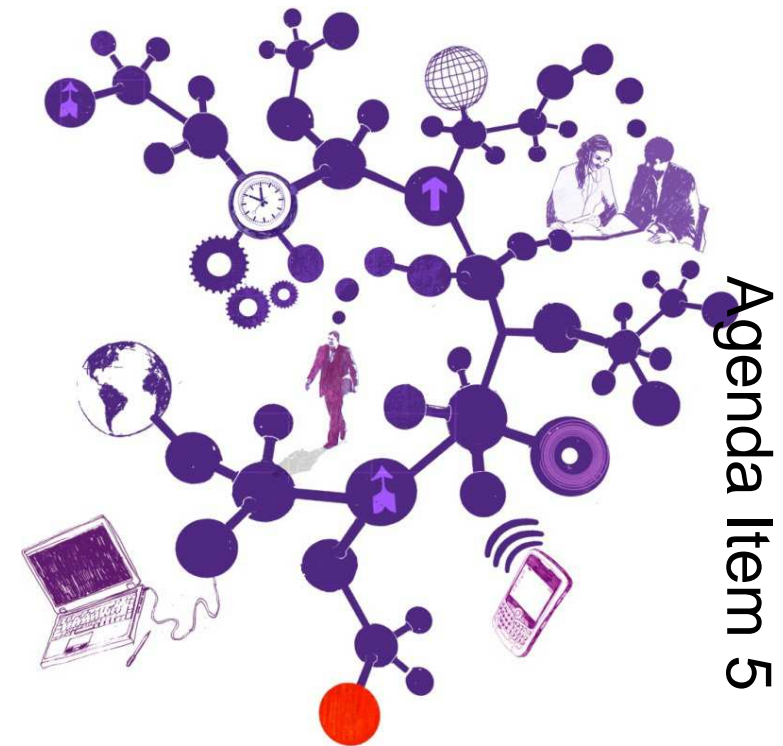
28 January 2016

Page 11

John Gregory
Director and Engagement Lead
T +44 (0)121 232 5333
E john.gregory@uk.gt.com

Joan Barnett
Manager
T +44 (0)121 232 5399
E joan.m.barnett@uk.gt.com

Denise Mills
In charge auditor
T +44 (0) 121 232 5306
E denise.f.mills@uk.gt.com



Agenda Item 5

The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our audit process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect your business or any weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Contents

Section	Page
Introduction	4
Progress at 28 January 2016	5
Emerging issues and developments	
Grant Thornton	8
Local government issues	14
Accounting and audit issues	17

Introduction

This paper provides the Audit and Governance Committee with a report on progress in delivering our responsibilities as your external auditors. The paper also includes:

- a summary of emerging national issues and developments that may be relevant to you; and
- a number of challenge questions in respect of these emerging issues which the Committee may wish to consider.

Members of the Audit and Governance Committee can find further useful material on our website www.grant-thornton.co.uk, where we have a section dedicated to our work in the public sector (<http://www.grant-thornton.co.uk/en/Services/Public-Sector/>). Here you can download copies of our publications including:

- Making devolution work: A practical guide for local leaders
- Spreading their wings: Building a successful local authority trading company
- Easing the burden, our report on the impact of welfare reform on local government and social housing organisations
- All aboard? our local government governance review 2015

If you would like further information on any items in this briefing, or would like to register with Grant Thornton to receive regular email updates on issues that are of interest to you, please contact either your Engagement Lead or Audit Manager. Their contact details are provided on the first page of this report.

Progress at 28 January 2016

Work	Planned date	Complete?	Comments
<p>2015-16 Accounts Audit Plan We are required to issue a detailed accounts audit plan to the Council setting out our proposed approach in order to give an opinion on the Council's 2015-16 financial statements.</p>	31 March 2016	In progress	
<p>Interim accounts audit Our interim fieldwork visit includes:</p> <ul style="list-style-type: none"> • updating our review of the Council's control environment • updating our understanding of financial systems • review of Internal Audit reports on core financial systems • early work on emerging accounting issues • early substantive testing • proposed Value for Money conclusion. 	The week commencing 25 January 2016 and the period 14 to 24 March 2016	In progress	We intend to complete early substantive testing up to February 2016. This will help ensure a smooth audit during the summer.
<p>2015-16 final accounts audit Including:</p> <ul style="list-style-type: none"> • audit of the 2015-16 financial statements • proposed opinion on the Council's accounts • proposed Value for Money conclusion. 	Timing of the audit to be confirmed as at the time of writing this report (19 January 2016)	Not yet started	

Progress at 28 January 2016

Work	Planned date	Complete?	Comments
<p>Value for Money (VfM) conclusion</p> <p>The scope of our work to inform the 2015/16 VfM conclusion has recently been subject to consultation from the National Audit Office. The audit guidance on the auditor's work on value for money arrangements was published on 9 November 2015.</p> <p>Auditors are required to reach their statutory conclusion on arrangements to secure VfM based on the following overall evaluation criterion: <i>In all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.</i></p> <p>To help auditors to consider this overall evaluation criterion, the following sub-criteria are intended to guide auditors in reaching their overall judgements:</p> <ul style="list-style-type: none"> • Informed decision making • Sustainable resource deployment • Working with partners and other third parties. <p>We are required to provide a conclusion that in all significant respects the Council has (or has not) put in place proper arrangements to secure value for money through economic, efficient and effective use of its resources for the 2015/16 period.</p>	<p>January onwards</p>	<p>In progress</p>	<p>The guidance and supporting information includes:</p> <ul style="list-style-type: none"> • the legal and professional framework; • definitions of what constitute 'proper arrangements'; • guidance on the approach to be followed by auditors in relation to risk assessment, with auditors only required to carry out detailed work in areas where significant risks have been identified; • evaluation criteria to be applied; • reporting requirements; • Council specific guidance. <p>The guidance is available at https://www.nao.org.uk/code-audit-practice/guidance-and-information-for-auditors/</p> <p>Now that the finalised auditor guidance is available, we will carry out an initial risk assessment to determine our approach and report this in our Audit Plan.</p> <p>Our work will be reported in the Audit Findings Report presented to the relevant Summer meeting of the Audit and Governance Committee (dates not yet set for the municipal year commencing 1 April 2016).</p>

Progress at 28 January 2016

Work	Planned date	Complete?	Comments
Other areas of work We are required to certify claims and returns per the directions issued by Public Sector Audit Appointments Limited in conjunction with the central government organisations providing the funding.	In line with the deadlines agreed with the sponsoring bodies	In progress	A meeting is scheduled with the Head of Benefits on 27 January 2016 to commence planning for this work.

Making devolution work: A practical guide for local leaders

Grant Thornton market insight

Our latest report on English devolution is intended as a practical guide for areas and partnerships making a case for devolved powers or budgets.

The recent round of devolution proposals has generated a huge amount of interest and discussion and much progress has been made in a short period of time. However, it is very unlikely that all proposals will be accepted and we believe that this the start of an iterative process extending across the current Parliament and potentially beyond.

With research partner Localis we have spent recent months speaking to senior figures across local and central government to get under the bonnet of devolution negotiations and understand best practice from both local and national perspectives. We have also directly supported the development of devolution proposals. In our view there are some clear lessons to learn about how local leaders can pitch successfully in the future.

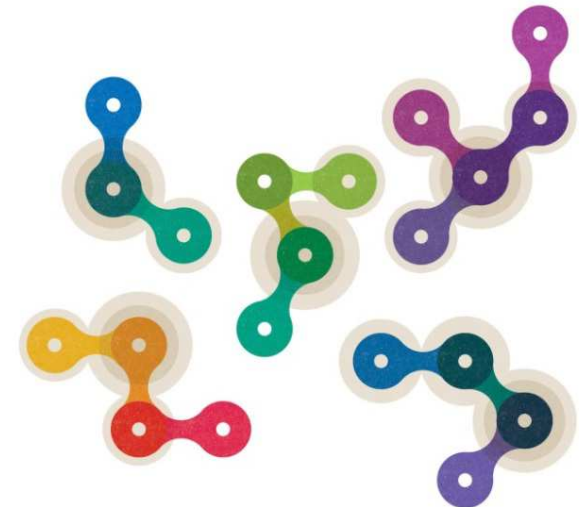
In particular, our report seeks to help local leaders think through the fundamental questions involved:

- what can we do differently and better?
- what precise powers are needed and what economic geography will be most effective?
- what governance do we need to give confidence to central government

The report 'Making devolution work: A practical guide for local leaders' can be downloaded from our website:

<http://www.grantthornton.co.uk/en/insights/making-devolution-work/>

Hard copies of our report are available from your Engagement Lead and Audit Manager



Turning up the volume: The Business Location Index

Grant Thornton market insight

Inward investment is a major component of delivering growth, helping to drive GDP, foster innovation, enhance productivity and create jobs, yet the amount of inward investment across England is starkly unequal.

The Business Location Index has been created to help local authorities, local enterprise partnerships, central government departments and other stakeholders understand more about, and ultimately redress, this imbalance. It will also contribute to the decision-making of foreign owners and investors and UK firms looking to relocate.

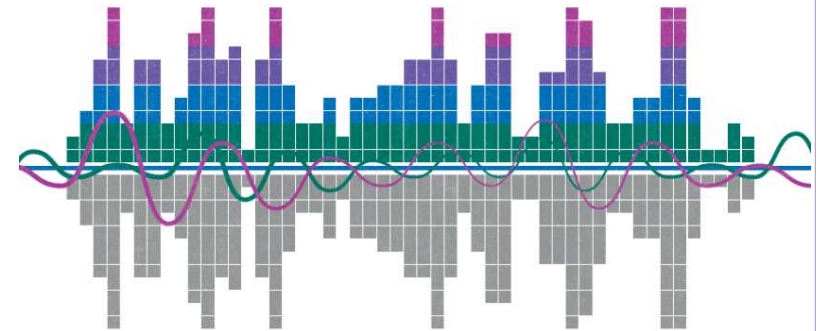
Based on in-depth research and consultation to identify the key factors that influence business location decisions around economic performance, access to people and skills and the environmental/infrastructure characteristics of an area, the Business Location Index ranks the overall quality of an area as a business location. Alongside this we have also undertaken an analysis of the costs of operating a business from each location. Together this analysis provides an interesting insight to the varied geography that exists across England, raising a number of significant implications for national and local policy makers.

At the more local level, the index helps local authorities and local enterprise partnerships better understand their strengths and assets as business locations. Armed with this analysis, they will be better equipped to turn up the volume on their inward investment strategy, promote their places and inform their devolution discussions.

The report 'Turning up the volume: The Business Location Index' can be downloaded from our website:

<http://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/publication/2015/business-location-index-turning-up-the-volume.pdf>

Hard copies of our report are available from your Engagement Lead and Audit Manager



Growing healthy communities: The Health and wellbeing index

Grant Thornton market insight

Our Place Analytics team reveals how collaboration between local authority stakeholders can help address health quality determinants (social, economic and environmental) and result in improved health outcomes (quality of lifestyle and health conditions).

It has long been recognised that the health of a population is strongly linked to the circumstances in which people live. Our index assesses 33 key health determinants and outcomes of health for the 324 English local authorities, to provide a coherent, national story on health and wellbeing. It highlights the scale and nature of inequality across the country and reiterates the need for a local, place-based approach to tackling health outcomes.

The purpose of this report is to help stakeholders – NHS providers and clinical commissioning groups (CCGs), local authorities, health and social care providers, housing associations, fire authorities and the police – to improve collaboration through a better understanding of the correlation between the economic, social and environmental health determinants and the health outcomes within their locality. It includes a concluding checklist of questions to help facilitate discussions in the light of joint service needs assessments.

The data behind the index also allows segmentation which reveals areas around the country with similar health determinants, but better outcomes. This underscores the need to work in collaboration with peers that may not be 'next door' if there is an opportunity to learn from 'others like us'.

Our report, Growing healthy communities: Health and Wellbeing Index, can be downloaded from our website: <http://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/publication/2015/growing-healthy-communities-health-and-wellbeing-index.pdf>

Hard copies of our report are available from your Engagement Lead and Audit Manager



Reforging local government

Summary findings of financial health checks and governance reviews

Grant Thornton market insight

The recent autumn statement represents the biggest change in local government finance in 35 years. The Chancellor announced that in 2019/20 councils will spend the same in cash terms as they do today and that "better financial management and further efficiency" will be required to achieve the projected 29% savings. Based on our latest review of financial resilience at English local authorities, this presents a serious challenge to many councils that have already become lean.

Our research suggests that:

- the majority of councils will continue to weather the financial storm, but to do so will now require difficult decisions to be made about services

Page 21
most councils project significant funding gaps over the next three to five years, but the lack of detailed plans to address these deficits in the medium-term represents a key risk

- Whitehall needs to go further and faster in allowing localities to drive growth and public service reform including proper fiscal devolution that supports businesses and communities
- local government needs a deeper understanding of their local partners to deliver the transformational changes that are needed and do more to break down silos
- elected members have an increasingly important role in ensuring good governance is not just about compliance with regulations, but also about effective management of change and risk
- councils need to improve the level of consultation with the public when prioritising services and make sure that their views help shape council development plans.



Supporting members in governance

Grant Thornton and the Centre for Public Scrutiny

We have teamed up with the Centre for Public Scrutiny to produce a member training programme on governance. Elected members are at the forefront of an era of unprecedented change, both within their own authority and increasingly as part of a wider local public sector agenda. The rising challenge of funding reductions, the increase of alternative delivery models, wider collaboration with other organisations and new devolution arrangements mean that there is a dramatic increase in the complexity of the governance landscape.

Members at local authorities – whether long-serving or newly elected – need the necessary support to develop their knowledge so that they achieve the right balance in their dual role of providing good governance while reflecting the needs and concerns of constituents.

To create an effective and on-going learning environment, our development programme is based around workshops and on-going coaching. The exact format and content is developed with you, by drawing from three broad modules to provide an affordable solution that matches the culture and the specific development requirements of your members.

- Module 1 – supporting members to meet future challenges
- Module 2 – supporting members in governance roles
- Module 3 – supporting leaders, committee chairs and portfolio holders

The development programme can begin with a baseline needs assessment, or be built on your own understanding of the situation.

Further details are available from your Engagement Lead and Audit Manager



Knowing the Ropes – Audit Committee Effectiveness Review

Grant Thornton

This is our first cross-sector review of audit committee effectiveness encompassing the corporate, not for profit and public sectors. It provides insight into the ways in which audit committees can create an effective role within an organisation's governance structure and understand how they are perceived more widely. It is available at <http://www.grantthornton.co.uk/en/insights/knowning-the-ropes--audit-committee-effectiveness-review-2015/>

The report is structured around four key issues:

- What is the status of the audit committee within the organisation?
- How should the audit committee be organised and operated?
- What skills and qualities are required in the audit committee members?
- How should the effectiveness of the audit committee be evaluated?

It raises key questions that audit committees, board members and senior management should ask themselves to challenge the effectiveness of their audit committee.

Our key messages are summarised opposite.



Size: 3-5 members is an ideal size for an audit committee

Frequency: meetings should be regular and the length should adapt to content

Relevance: audit committee members should be selected based on the skills and experience they bring

Communication: papers should strike the balance between detail and length

Ability: training should be provided for audit committee members

Clarity: the role of the audit committee and its relationship with other committees, should be clearly defined

Evolution: audit committees should continually develop

The two key things that audit committee members should be asking are:

- 1 What is expected of the audit committee and does it reflect the specific nature of the industry in which the organisation sits?
- 2 Does the audit committee have clear terms of reference in place? Audit committees should set themselves targets for what they want to achieve and define how these will be measured to ensure they are operating effectively.

George Osborne sets out plans for local government to gain new powers and retain local taxes

Local government issues

The Chancellor unveiled the "devolution revolution" on 5 October 2015 involving major plans to devolve new powers from Whitehall to Local Government. Local Government will now be able to retain 100 per cent of local taxes and business rates to spend on local government services; the first time since 1990. This will bring about the abolition of uniform business rates, leaving local authorities with the power to cut business rates in order to boost enterprise and economic activity within their areas. However, revenue support grants will begin to be phased out and so local authorities will have to take on additional responsibility. Elected Mayors, with the support of local business leaders in their LEPs, will have the ability to add a premium to business rates in order to fund infrastructure, however this will be capped at 2 per cent.

There has been a mixed reaction to this announcement. Some commentators believe that this will be disastrous for authorities which are too small to be self-sufficient. For these authorities, the devolution of powers and loss of government grants will make them worse off. It has also been argued that full devolution will potentially drive up council's debt as they look to borrow more to invest in business development, and that this will fragment the creditworthiness of local government.

Challenge question

Have members:

- been briefed by your Executive Director (Corporate Services) on the Chancellor's "devolution revolution" announcement and its likely impact on the Council?

Councils must deliver local plans for new homes by 2017

Local government issues

The Prime Minister announced on 12 October 2015 that all local authorities must have plans for the development of new homes in their area by 2017, otherwise central government will ensure that plans are produced for them. This will help achieve government's ambition of 1 million more new homes by 2020, as part of the newly announced Housing and Planning Bill.

The government has also announced a new £10 million Starter Homes fund, which all local authorities will be able to bid for. The Right to Buy Scheme has been extended with a new agreement with Housing Associations and the National Housing Federation. The new agreement will allow a further 1.3 million families the right to buy, whilst at the same time delivering thousands of new affordable homes across the country. The proposal will increase home ownership and boost the overall housing supply. Housing Association tenants will have the right to buy the property at a discounted rate and the government will compensate the Housing Associate for their loss.

Challenge question

Have members:

- been briefed by your Executive Director (Corporate Services) on the government's new homes announcements and their likely impact on the Council?

Improving efficiency of council tax collection

Local government issues

DCLG have published "Improving Efficiency for Council Tax Collection", calling for consultation on the proposals to facilitate improvements in the collection and enforcement processes in business rates and council tax. The consultation is aimed specifically at local authorities, as well as other government departments, businesses and any other interested parties. The consultation document states that council tax collection rates in 2014-15 are generally high (at 97 per cent), however the government wishes to explore further tools for use by local authorities and therefore seeks consultation from local authorities on DCLG's proposals. The consultation closes on 18 November.

The Government proposes to extend the data-sharing gateway which currently exists between HMRC and local authorities. Where a liability order has been obtained, the council taxpayer will have 14 days to voluntarily share employment information with the council to enable the council to make an attachment to earnings. If this does not happen, the Government proposes to allow HMRC to share employment information with councils. This would help to avoid further court action, would provide quicker access to reliable information, and would not impose any additional costs on the debtor. The principle of this data-sharing is already well-established for council taxpayers covered by the Local Council Tax Support scheme, and it would make the powers applying to all council tax debtors consistent. Based on the results of the Manchester/HMRC pilot, Manchester estimate that £2.5m of debt could potentially be recouped in their area alone.

Challenge question

Have members:

- been briefed by your Executive Director (Corporate Services) on the government's council tax collection consultation and the Council's response to it?

Code of Audit Practice

National Audit Office

Under the Local Audit and Accountability Act 2014 the National Audit Office are responsible for setting the Code of Audit Practice which prescribes how local auditors undertake their functions for public bodies, including local authorities.

The NAO have published the Code of Audit Practice which applies for the audit of the 2015/16 financial year onwards. This is available at <https://www.nao.org.uk/code-audit-practice/wp-content/uploads/sites/29/2015/03/Final-Code-of-Audit-Practice.pdf>

The Code is principles based and will continue to require auditors to issue:

- Opinion on the financial statements
- Opinion on other matters
- Opinion on whether the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources (the "VFM conclusion".)

The NAO has supplemented the new Code with detailed auditor guidance in specific areas. The audit guidance on the auditor's work on value for money arrangements was published on 9 November 2015. The guidance includes the following.

- The legal and professional framework
- Definitions of what constitute "proper arrangements" for securing economy, efficiency and effectiveness in the use of resources
- Guidance on the approach to be followed by auditors in relation to risk assessment, with auditors only required to carry out detailed work in areas where significant risks have been identified
- Evaluation criteria to be applied
- Reporting requirements.

Guidance Note AGN03 is available at <https://www.nao.org.uk/code-audit-practice/wp-content/uploads/sites/29/2015/03/Auditor-Guidance-Note-03-VFM-Arrangements-Work-09-11-15.pdf>



© 2016 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton is a member firm of Grant Thornton International Ltd (Grant Thornton International). References to 'Grant Thornton' are to the brand under which the Grant Thornton member firms operate and refer to one or more member firms, as the context requires. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by member firms, which are not responsible for the services or activities of one another. Grant Thornton International does not provide services to clients.

grant-thornton.co.uk

AUDIT & GOVERNANCE COMMITTEE

28th January 2016

Report of the Head of Internal Audit Services

INTERNAL AUDIT ANNUAL REPORT/QUARTERLY REPORT 2015/16 QUARTER 3

EXEMPT INFORMATION

None

PURPOSE

To report on the outcome of Internal Audit's review of the internal control, risk management and governance framework in the 3rd quarter of 2015/16 – to provide members with assurance of the ongoing effective operation of an internal audit function and enable any particularly significant issues to be brought to the Committee's attention.

RECOMMENDATION

That the Committee considers the attached quarterly report and raises any issue it deems appropriate.

EXECUTIVE SUMMARY

The Accounts and Audit Regulations 2011 (as amended) require each local authority to publish an Annual Governance Statement (AGS) with its Annual Statement of Accounts. The AGS is required to reflect the various arrangements within the Authority for providing assurance on the internal control, risk management and governance framework within the organisation, and their outcomes.

One of the sources of assurance featured in the AGS is the professional opinion of the Head of Internal Audit Services on the outcome of service reviews. Professional good practice recommends that this opinion be given periodically throughout the year to inform the Annual Governance Statement. This opinion is given on a quarterly basis to the Audit & Governance Committee.

The Head of Internal Audit Services' quarterly opinion statement for Oct – Dec 2015 (Qtr 3) is set out in the attached document, and the opinion is summarised below.

Based on the ongoing work carried out by and on behalf of Internal Audit and other sources of information and assurance, my overall opinion of the control environment for this quarter is that "reasonable assurance" can be given.

Where significant deficiencies in internal control have been formally identified by management, Internal Audit or by external audit or other agencies, management have given assurances that these have been or will be resolved in an appropriate manner. Such cases will continue to be monitored. Internal Audit's opinion is one of the sources of assurance for the Annual Governance Statement which is statutorily required to be presented with the annual Statement of Accounts.

Specific Issues

No specific issues have been highlighted through the work undertaken by Internal Audit during 2015/16.

RESOURCE IMPLICATIONS

None

LEGAL/RISK IMPLICATIONS

Failure to report would lead to non-compliance with the requirements of the Annual Governance Statement and the Public Sector Internal Audit Standards.

SUSTAINABILITY IMPLICATIONS

None

BACKGROUND INFORMATION

None

REPORT AUTHOR

Angela Struthers, Head of Internal Audit Services

LIST OF BACKGROUND PAPERS

None

APPENDICES

- Appendix 1 Internal Audit Performance Report 2015/16 Quarter 3
- Appendix 2 Percentage of Management Actions Agreed 2015/16 Quarter 3
- Appendix 3 Implementation of Agreed Management Actions 2015/16

INTERNAL AUDIT ANNUAL REPORT/QUARTERLY REPORT – Q3 - 2015/16

1. INTRODUCTION

Internal Audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. (Public Sector Internal Audit Standards)

Internal Audit's role is to provide independent assurance to the Council that systems are in place and are operating effectively.

Every local authority is statutorily required to provide for an adequate and effective internal audit function. The Internal Audit service provides this function at this Authority.

This brief report aims to ensure that Committee members are kept aware of the arrangements operated by the Internal Audit service to monitor the control environment within the services and functions of the authority, and the outcome of that monitoring. This is to contribute to corporate governance and assurance arrangements and ensure compliance with statutory and professional duties, as Internal Audit is required to provide periodic reports to "those charged with governance".

2. PERFORMANCE AND PROGRESSION AGAINST AUDIT PLAN

The Internal Audit service aims as one of its main Performance Indicators (PI's) to complete work on at least 90% of applicable planned audits by the end of the financial year, producing draft reports on these where possible/necessary. **Appendix 1** shows the progress at the end of quarter 3 of the work completed against the plan and highlights the work completed in the third quarter. At the end of the third quarter, internal audit have started/completed 40 areas of work from the 2015/16 audit plan which equates to 72% of the revised annual plan. We have completed work in one additional area that was unplanned and have to cancel three audit reviews at management's request.

The service also reports quarterly on the percentage of draft reports issued within 15 working days of the completion of fieldwork. All (100%) of the draft reports issued in this quarter of the year were issued within this deadline.

3. AUDIT REVIEWS COMPLETED QUARTER 3 2015/16

Appendix 2 details the number of recommendations made. A total of 55 recommendations were made in the third quarter with 55 (100%) of the recommendations being accepted by management.

The service revisits areas it has audited around 6 months after agreeing a final report on the audit, to test and report to management on the extent to which agreed actions have been taken. Six implementation reviews were completed during the 3rd quarter of 2015/16. **Appendix 3** details the implementation reviews completed showing the revised assurance levels. The implementation reviews completed identified that 59% of the agreed management actions were implemented or partially implemented.

Internal Audit is fairly satisfied with the progress made by management to reduce the level of risk and its commitment to progressing the outstanding issues. As there are still a number of high priority actions still requiring to be completed, additional implementation reviews will be carried out to ensure the implementation of the actions is completed.

4. INDEPENDENCE OF THE INTERNAL AUDIT ACTIVITY

Attribute Standards 1110 to 1130 in the Public Sector Internal Audit Standards require that Internal Audit have organisational and individual independence and specifically states that the head of Internal Audit Services must confirm this to the Audit & Governance Committee at least annually. As performance is reported quarterly, this confirmation will be provided quarterly.

The Head of Internal Audit Services confirms that Internal Audit is operating independently of management and is objective in the performance of internal audit work.

5 OVERALL CURRENT INTERNAL AUDIT OPINION

Based on the ongoing work carried out by and on behalf of Internal Audit and other sources of information and assurance, my overall opinion of the Governance, risk and control environment at this time is that “reasonable assurance” can be given. Where significant deficiencies in internal control have been formally identified by management, Internal Audit or by external audit or other agencies, management have given assurances that these have been or will be resolved in an appropriate manner. Such cases will continue to be monitored. Internal Audit’s opinion is one of the sources of assurance for the Annual Governance Statement which is statutorily required to be presented with the annual Statement of Accounts.

Specific issues:

There were no specific issues highlighted through the work of Internal Audit in the third quarter of the 2015/16 financial year

Angela Struthers,
Head of Internal Audit Services

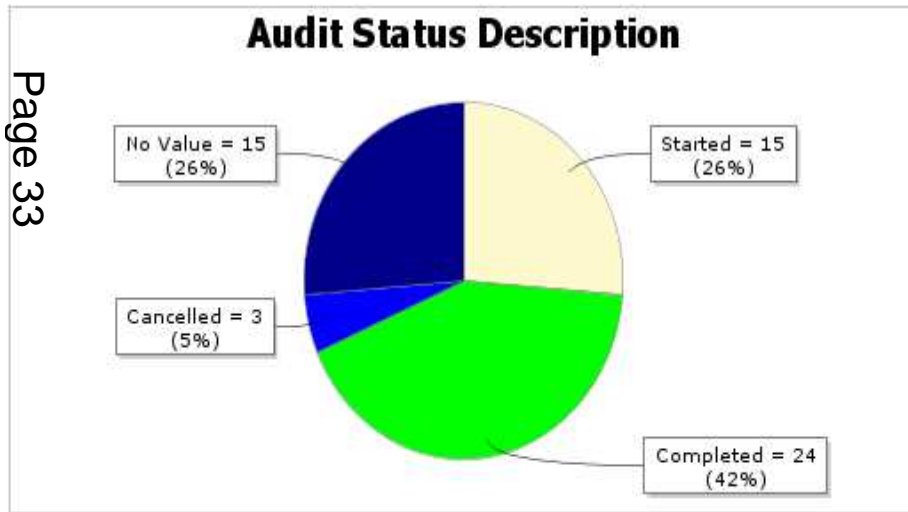


Internal Audit Performance Report 2015/16 Quarter 3

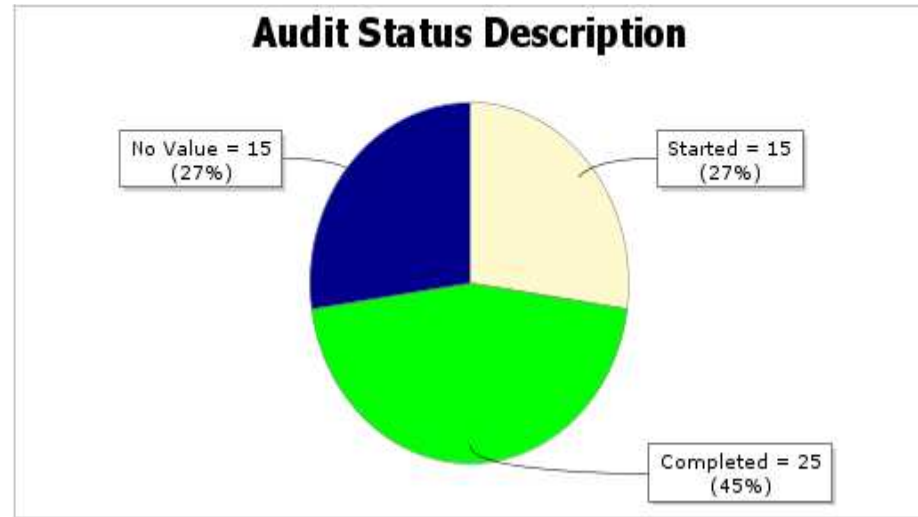
Report Type: Audit File Report
 Report Author: Angela Struthers
 Generated on: 21 December 2015

Page 33

Original Plan



Revised Plan



Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title
Treasury Management Qtr3 2015/16	Finance			Main financial system – interim
Council Tax	Finance	✓	Completed	Main financial system – interim

Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title
NNDR	Finance	✓	Completed	Main financial system – interim
Bank Reconciliation & Cash Collection	Finance	✓	Completed	Main financial system – interim
Housing Rents	Housing & Health	✓	Started	Main financial system – interim
Debtors	Finance	✓	Started	Main financial system – interim
Main Accounting & Budgetary Control	Finance	✓	Started	Main financial system – interim
Capital Strategy & Programme Management	Finance			Main financial system – interim
Housing Anti-Social Behaviour	Housing & Health	✓	Completed	Risk based review
Debtors & Procurement	Finance	✓	Started	Main financial system – interim
Housing & Council Tax Benefits	Finance	✓	Completed	Main financial system – interim
Payroll	Transformation & Corporate Performance			Main financial system – interim
Housing Repairs QTR 2	Housing & Health	✓	Completed	Main financial system – interim
Housing Repairs QTR 4	Housing & Health			Main financial system – interim
Property Contracts QTR 2	Assets & Environment	✓	Completed	Main financial system – interim
Property Contracts QTR 3	Assets & Environment	✓	Started	Main financial system – interim
Municipal Charities	Corporate	✓	Completed	Transactional
I Trent	Technology & Corporate Programmes	✓	Started	Information Technology
Pension Contributions	Transformation & Corporate Performance	✓	Completed	Compliance
Housing Repairs QTR 1	Housing & Health	✓	Completed	Main financial system – interim

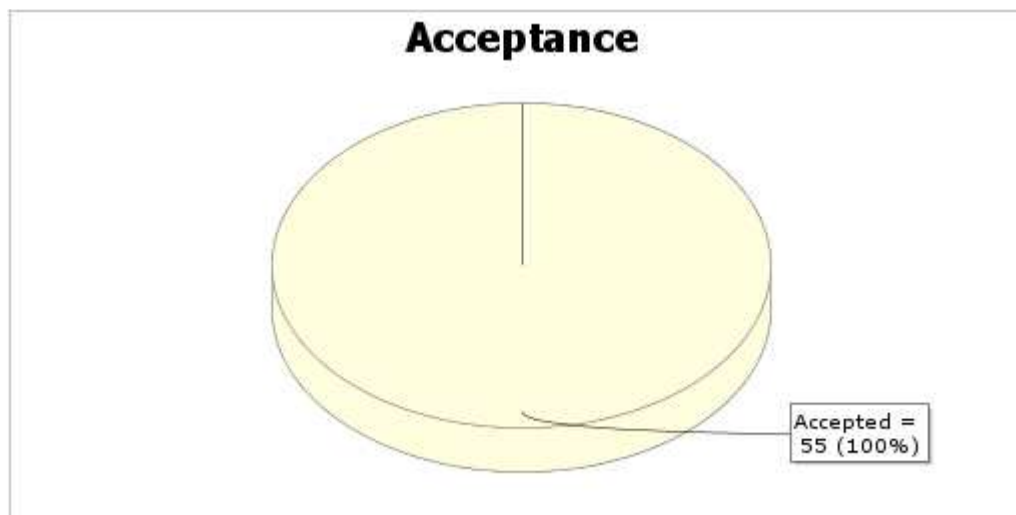
Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title
Housing Repairs QTR 3	Housing & Health	✓	Started	Main financial system – interim
Property Contracts QTR 1	Assets & Environment	✓	Completed	Main financial system – interim
Property Contracts QTR 4	Assets & Environment			Main financial system – interim
Treasury Management Qtr4 2014/15	Finance	✓	Completed	Main financial system – interim
Treasury Management Qtr1 2015/16	Finance	✓	Completed	Main financial system – interim
Treasury Management Qtr2 2015/16	Finance	✓	Completed	Main financial system – interim
Transparency Code	Corporate	✓	Completed	Compliance
Safeguarding Children & Vulnerable Adults	Solicitor & Monitoring Officer	✓	Completed	System based review
Assembly Rooms Bar	Communities, Planning & Partnerships	✓	Started	System based review
Housing Voids & Lettings	Housing & Health	✓	Completed	System based review
IT Governance	Technology & Corporate Programmes	●	Cancelled	Consultancy
Performance Framework	Transformation & Corporate Performance			Consultancy
Alternative Delivery Models	Corporate	✓	Started	System based review
Assembly Rooms Project	Communities, Planning & Partnerships			Consultancy
Electoral Process	Solicitor & Monitoring Officer			System based review
Asbestos & Legionella	Assets & Environment	✓	Completed	Risk based review
Recruitment Process	Transformation & Corporate	✓	Completed	System based review

Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title
	Performance			
Planning Enforcement	Communities, Planning & Partnerships	✔	Completed	Risk based review
Community Safety/ Development	Communities, Planning & Partnerships	●	Cancelled	System based review
Transformation process/ Corporate Change	Corporate			System based review
Review of Culture/ Ethics	Corporate	✔	Started	Consultancy
RIPA	Solicitor & Monitoring Officer	✔	Started	Compliance
Customer Services	Transformation & Corporate Performance			Risk based review
Corporate Complaints/ Service Feedback	Transformation & Corporate Performance	✔	Started	System based review
Corporate Business Continuity	Technology & Corporate Programmes			System based review
Car Parking	Assets & Environment			Risk based review
Taxi/PHV Licences	Assets & Environment	✔	Started	System based review
Private Sector Housing Leasing Scheme	Housing & Health			System based review
Telephony Project Implementation Review	Technology & Corporate Programmes			Information Technology
IT Disaster Recovery	Technology & Corporate Programmes	✔	Started	Information Technology
DIP Application Review	Technology & Corporate Programmes			Information Technology
IT Governance Review	Technology & Corporate	●	Cancelled	Information Technology

Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title
	Programmes			
Organisational Development	Transformation & Corporate Performance	✔	Completed	Risk based review
Homelessness	Housing & Health	✔	Completed	Risk based review
Commercial & Industrial Properties	Assets & Environment	✔	Started	Consultancy
Electoral Registration/Canvassing Process	Solicitor & Monitoring Officer	✔	Completed	System based review
M3 Application Review	Technology & Corporate Programmes	✔	Completed	Information Technology
Additional Pensions Contributions Review	Transformation & Corporate Performance	✔	Completed	Transactional – Additional

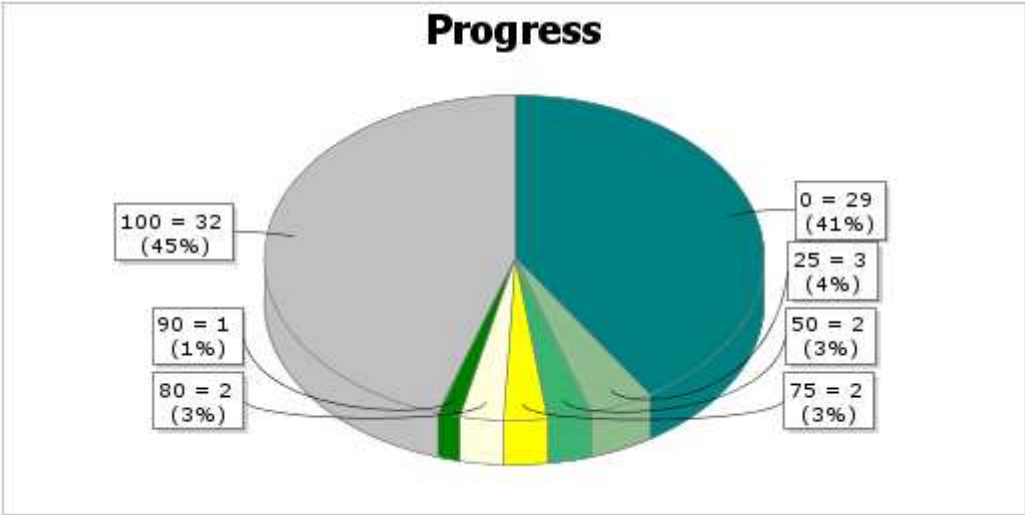
This page is intentionally left blank

Percentage of Management Actions Agreed 2015/16 Quarter 3




















This page is intentionally left blank








Implementation of Agreed Management Actions 2015/16 Quarter 3



Page 41

Audit Recommendation Code & Title	Audit Recommendation Status Icon	Audit Recommendation Priority	Audit Recommendation Progress Bar	Audit Recommendation Reasons Not Implemented Description
1314 Orch 1.1 Passwords	✓	High Priority	0%	Reliance on 3rd Party – Internal
1314 Orch 1.2 Generic user accounts	✓	High Priority	0%	Other Higher Priorities
1314 Orch 1.3 System Administrator User Access	✓	High Priority	0%	Other Higher Priorities
1314 S106 1.1 Procedures	✓	High Priority	0%	Staffing Resources – Temporary
1314 S106 2.1 Financial	✓	High Priority	0%	Staffing Resources – Temporary

Audit Recommendation Code & Title	Audit Recommendation Status Icon	Audit Recommendation Priority	Audit Recommendation Progress Bar	Audit Recommendation Reasons Not Implemented Description
1314 S106 3.1 Database		High Priority	<input type="text" value="0%"/>	Staffing Resources – Temporary
1415 DP 03 Confidential Waste Disposal Contract		High Priority	<input type="text" value="0%"/>	Reliance on 3rd Party – Internal
1415 IT IC 01 Policies		High Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 11 Secure emails		High Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 12 Procedure review		High Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 14 Passwords		High Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 16 Review of firewall rules		High Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 LSR 03 Contracts		High Priority	<input type="text" value="0%"/>	Other Higher Priorities
1314 Orch 1.4 Review of Users		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1314 S106 1.2 Monitoring		Medium Priority	<input type="text" value="0%"/>	Staffing Resources – Temporary
1415 DP 01 Data Protection Risk Register		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 DP 01 Policy Issue		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 DP 03 Business Continuity Arrangements		Medium Priority	<input type="text" value="0%"/>	Reliance on 3rd Party – Internal
1415 DP 03 Confidential Waste Bins		Medium Priority	<input type="text" value="0%"/>	Reliance on 3rd Party – Internal
1415 DP 03 Records of Off Site Storage Facilities		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 DP 04 Security Policies		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 DP 05 Requests for Personal		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities

Audit Recommendation Code & Title	Audit Recommendation Status Icon	Audit Recommendation Priority	Audit Recommendation Progress Bar	Audit Recommendation Reasons Not Implemented Description
Data				
1415 DP 07 Data Protection Notification		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 DP 08 Privacy Notices		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 02 User Responsibilities		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 06 Review of permissions		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 IT IC 15 Firewall procedures		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities
1415 Xpress 2.01 Change Management & Development Plan		Medium Priority	<input type="text" value="0%"/>	Reliance on 3rd Party – Internal
1415 Xpress 3.01 Service Reviews and Support		Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities

This page is intentionally left blank

AUDIT AND GOVERNANCE COMMITTEE

28th January 2016

REPORT OF THE HEAD OF INTERNAL AUDIT SERVICES

RISK MANAGEMENT UPDATE 2015/16

EXEMPT INFORMATION

None

PURPOSE

To report on the Risk Management process and progress to date for the current financial year.

RECOMMENDATIONS

That the Committee:

- 1 Endorses the Corporate Risk Register 2015/16, and**
- 2 Endorses the Risk Management Action Plan 2015/16**

EXECUTIVE SUMMARY

One of the functions of the Audit & Governance Committee is to monitor the effectiveness of the authority's risk management arrangements, including the actions taken to manage risks and to receive regular reports on risk management. Corporate risks are identified and managed and monitored by the Corporate Management Team (CMT) on a quarterly basis. Corporate risks have been assigned to relevant members of the Corporate Management Team. Through regular review, risks may be added or removed from the Corporate Risk Register. The Corporate Risk Register is attached as **Appendix 1** for information.

Work is continually completed by Internal Audit with Service Units to ensure that the operational risk register entries are aligned to the corporate risks. This will also identify areas where operational risk registers need to be updated to ensure that operationally, the corporate risks are managed. The Risk Management Action Plan for 2015/16 is attached as **Appendix 2** and shows status to date.

RESOURCE IMPLICATIONS

None

LEGAL/RISK IMPLICATIONS BACKGROUND

None

SUSTAINABILITY IMPLICATIONS

None

BACKGROUND INFORMATION

None

REPORT AUTHOR

Angela Struthers, Head of Internal Audit Services ex 234

LIST OF BACKGROUND PAPERS

None

APPENDICES

Appendix 1 – Corporate Risk Register 2015/16

Appendix 2 – Risk Management Action Plan 2015/16



Risk Management Action Plan 2015/16

Report Type: Actions Report

Report Author: Angela Struthers

Generated on: 24 December 2015

Action Code	Action Title	Priority	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM1	Risk Management Policy	1		<div style="width: 100%;"><div style="background-color: #4f81bd; height: 10px; width: 100%;"></div></div> 100%	30-Sep-2015	03-Sep-2015	Angela Struthers
Description	Risk Management Policy Review						
All Notes	Angela Struthers 03-Sep-2015 Risk Management Policy reviewed and presented to the Audit & Governance Committee October 2015 Policy review timetable set up on Covalent						
	Angela Struthers 11-May-2015 The Risk Management Policy has been reviewed and updated and is currently in draft stage. Due to other work commitments, the formal review/adoption process has been delayed. Revised date September 2015						
	Angela Struthers 07-Aug-2014 The Policy will be reviewed by the due date						
Action Code	Action Title	Priority	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM2	Risk Management Training	2		<div style="width: 40%;"><div style="background-color: #4f81bd; height: 10px; width: 40%;"></div></div> 40%	31-Mar-2016		Angela Struthers
Description	Roll out e-learning risk management module						
All Notes	Angela Struthers 03-Sep-2015 Roll out of e-learning delayed - revised date 31 March 2016						
	Angela Struthers 11-May-2015 The risk management module has been developed and ready for issue. The software is in the process of being updated so this has delayed the issue of the module. Revised date September 2015						
Action Code	Action Title	Priority	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM3	E-learning module	2		<div style="width: 100%;"><div style="background-color: #4f81bd; height: 10px; width: 100%;"></div></div> 100%	01-Apr-2015	11-May-2015	Angela Struthers
Description	Review e-learning module to alarm toolkit						
All Notes	Angela Struthers 11-May-2015 Continuous review of the module is completed						

Action Code	Action Title	Priorit y	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM4	Linking risks to corporate priorities	2		50%	31-Mar-2016		Angela Struthers
Description	Linking risks to corporate priorities and statements of intent						
All Notes	Angela Struthers 03-Sep-2015 Completed through the audit/risk management process on a one to one basis Angela Struthers 03-Sep-2015 The Covalent system has been adapted so that this is now possible to complete, however, due to the delay in the roll out of training , this facility has not been bought to the attention of all users. Users are notified of this if they complete one to one training. Revised completion date September 2015						

Action Code	Action Title	Priorit y	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM5	Opportunities Risk Register	3		0%	01-Apr-2016		Angela Struthers
Description	Introduce an opportunities risk register						
All Notes	Angela Struthers 03-Sep-2015 Still awaiting software development - the suppliers are currently developing a browser based version of the software so additional development areas have been put on hold Angela Struthers 11-May-2015 Still awaiting software development Angela Struthers 07-Aug-2014 This is a development area. A request to the software supplier has been made.						

Action Code	Action Title	Priorit y	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM6	Internal Controls	3		75%	01-Apr-2016		Angela Struthers
Description	Evaluate the option to populate the Internal Controls tab within the Covalent Risk Management system						
All Notes	Angela Struthers 03-Sep-2015 Further review not yet due Angela Struthers 11-May-2015 This has been evaluated and will not be implemented at this time as there is no benefit at the moment. However, the situation will be reviewed in a further 12 months. Revised completion date April 2016						

Action Code	Action Title	Priorit y	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM7	Risk Library	2		100%	01-Apr-2015	14-Oct-2014	Angela Struthers
Description	Increase the Risk Management Library						
All Notes	Angela Struthers 07-Aug-2014 The risk library held on the covalent system now contains project and partnerships risk libraries as these are the areas that will be used by several departments. Other risk libraries are more specific to the service area and will remain as word documents.						

Action Code	Action Title	Priority	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM8	Health & Safety Risk Registers	2		<div style="width: 25%;"><div style="background-color: blue; height: 10px; width: 100%;"></div></div> 25%	01-Apr-2016		Angela Struthers
Description	Promote the use of Covalent Risk Management system to record health & safety risk registers						
All Notes	Angela Struthers 03-Sep-2015 Promotion of the system still on going Angela Struthers 11-May-2015 Promotion of the use of Covalent for the recording of health and safety risk registers has been completed and adopted in some areas in line with audits as they are completed. Further promotion will be completed as audits are completed. Revised completion date April 2016						

Action Code	Action Title	Priority	Current Status	Progress Bar	Due Date	Completed Date	Assigned To
RM9	Other Assurance Sources	3		<div style="width: 50%;"><div style="background-color: blue; height: 10px; width: 100%;"></div></div> 50%	01-Apr-2016		Angela Struthers
Description	To promote the recording of other assurance sources on the Covalent system						
All Notes	Angela Struthers 03-Sep-2015 Promotion of the recording of other assurance sources still ongoing Angela Struthers 11-May-2015 The Covalent system has been adapted so that this can be completed and as one to one training is completed it is highlighted. The facility will be highlighted during the training sessions. Revised completion date April 2016						

Page 49

Action Status	
	Cancelled
	Overdue; Neglected
	Unassigned; Check Progress
	Not Started; In Progress; Assigned
	Completed

This page is intentionally left blank

















Corporate Risk Register 2015/16

Report Type: Risks Report
Report Author: Angela Struthers
Generated on: 08 January 2016



Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Medium Term Financial Planning & Sustainability Strategy	Loss of Funding and Financial Stability.		12 major – likely		8 major – unlikely	08-Jan-2016
Reputation	Damage to Reputation		9 serious–likely		4 significant–unlikely	08-Jan-2016
Governance & Regulatory Failure	Failure to achieve adequate Governance Standards and statutory responsibilities		9 serious–likely		4 significant–unlikely	08-Jan-2016
Partnership Working and Supply Chain Challenges	Failure in partnership working, shared services or supply chain		9 serious–likely		4 significant–unlikely	08-Jan-2016
Emergency & Crisis Response Threats	Failure to manage an external or internal emergency/disaster situation		9 serious–likely		4 significant–unlikely	08-Jan-2016
Economic Changes	Failure to plan and adapt services to economic changes within the community		6 serious–unlikely		3 serious–very unlikely	08-Jan-2016
Information Management & Information Technology	Failure to secure and manage data and IT infrastructure		12 major – likely		6 serious–unlikely	08-Jan-2016

Page 51

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Loss of Community Cohesion	Failure to achieve community cohesion		12 major – likely		9 serious–likely	08-Jan-2016
Workforce Planning Challenges	Failure to manage workforce planning challenges		9 serious–likely		4 significant–unlikely	08-Jan-2016
Health & Safety	Failure to manage Health & Safety		12 major – likely		6 serious–unlikely	08-Jan-2016
Corporate Change	Failure to manage corporate change		4 significant–unlikely		4 significant–unlikely	08-Jan-2016
Safeguarding Children & Vulnerable Adults	Failure to safeguard children and vulnerable adults		12 serious – very likely		9 serious–likely	08-Jan-2016
Sale of land for housing – Amington	Cabinet selected to redevelop the Golf Course for housing following the in-depth options appraisal. Prior to this, Cabinet approved the closure of the course in October 2014. The project to redevelop the site is ongoing and a number of technical studies are being finalised. Outline planning permission approved 4 August 2015 – site to be marketed by September 2015.		12 serious – very likely		6 serious–unlikely	08-Jan-2016
Inability to manage the impact corporately of the Government Austerity measures and new legislative requirements	Inability to manage the impact corporately of the Government Austerity measures and new legislative requirements		16 major – very likely		8 major – unlikely	08-Jan-2016
Elections	Parliamentary & Local Elections 2016		9 serious–likely		4 significant–unlikely	08-Jan-2016

This page is intentionally left blank

AUDIT & GOVERNANCE COMMITTEE

28th January 2016

REPORT OF THE HEAD OF INTERNAL AUDIT SERVICES

FRAUD AND CORRUPTION UPDATE REPORT

EXEMPT INFORMATION

None

PURPOSE

To provide Members with an update of Counter Fraud work completed to date during the financial year 2015/16.

RECOMMENDATIONS

That the Committee:

- 1 Considers this report and raises any issue it deems appropriate,**
- 2 Endorses the Fraud Risk Register Summary (Appendix 1), and**
- 3 Endorses the assessment against the Code of Practice on Managing the Risk of Fraud and Corruption (Appendix 2).**

EXECUTIVE SUMMARY

The abolition of the National Fraud Authority in 2014 and the closure of the Audit Commission in 2015 saw professional counter fraud bodies, institutes and other concerned stakeholders from across the public and private sector including the former Counter Fraud Team of the Audit Commission come together to form 'The European Institute for Combating Corruption And Fraud' (TEICCAF). TEICCAF have carried on from the Audit Commission in the Protecting the Public Purse annual publications.

In line with good practice, a Fraud Risk Register is maintained and reviewed on a quarterly basis. The latest Fraud Risk Register Summary is attached as **Appendix 1**.

Work has progressed on the data matches identified through the National Fraud Initiative (NFI) in the 2014/15 run which was released in February 2015. In total, 1125 matches were identified with 234 of these being recommended for investigation by the Council. So far, 950 of the matches have been processed and closed and 7 remain in progress. All of the recommended matches have been investigated and closed. No frauds were identified but there were two errors uncovered, one relating to Housing Benefits with a value of £2110 and a duplicate invoice with a value of £733. Both errors have been corrected.

Following the move of the Housing Benefits Fraud Investigations to the Single Fraud Investigation Service at the Department of Works and Pensions, the Authority has a dedicated Corporate Anti Fraud Investigations Officer who has been in post since September 2015. This ensures that the Authority is taking a more proactive approach to fraud rather than a reactive approach previously adopted. As well as continuing with the work on the NFI matches previously identified and new matches as they are identified, the Corporate Anti Fraud Investigations Officer's current case load includes ongoing investigations into potential fraud in these areas - Council Tax Reduction, Single Persons Discount, illegal subletting of council housing and non-residence of council housing. Investigations concluded have identified three cases of fraudulent Single Persons Discount claims and one fraudulent Council Tax Reduction Scheme claim. Whilst the monetary value for these cases is known, the total fraud identified will be reported to this Committee at year end following appropriate guidance on the correct multiplier to apply to each type of case so that the outcomes can be correctly reported.

In accordance with good practice, we have measured ourselves against the CIPFA Code of Practice on Managing the Risk of Fraud & Corruption. Compliance with the Code of Practice is not mandatory. The Code of Practice identifies eighteen actions that are required to manage the risk of fraud. Of these eighteen actions, fifteen are complete. The areas requiring further action are the estimation of fraud loss for which we need to follow appropriate guidance on the correct multiplier to apply to each type of case so that outcomes can be correctly reported; the adoption of a Data & Intelligence Sharing Protocol to be completed by the Director – Technology & Corporate Programmes; and the completion of an Annual Report both of which are due at the end of the financial year. The assessment against the Code of Practice on Managing the Risk of Fraud and Corruption is attached as **Appendix 2**.

RESOURCES IMPLICATIONS

None

LEGAL/RISK IMPLICATIONS BACKGROUND

There is a risk that the Authority will not have sound governance processes in place.

SUSTAINABILITY IMPLICATIONS

None

BACKGROUND INFORMATION

None

REPORT AUTHOR

Angela Struthers ex 234

LIST OF BACKGROUND PAPERS

None

APPENDICES

- Appendix 1 - Fraud Risk Register Summary**
- Appendix 2 - Code of Practice on Managing the Risk of Fraud & Corruption**

This page is intentionally left blank
























Fraud Risk Register Summary



















Report Type: Risks Report
Report Author: Angela Struthers
Generated on: 14 January 2016




Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Staffing (internal)						
Credit Income	Misappropriation of income		4 significant–unlikely		2 significant–very unlikely	25–Nov–2015
Assets	Theft of fixed assets		9 serious–likely		4 significant–unlikely	25–Nov–2015
Assets	Theft of Council information/intellectual property		12 major – likely		8 major – unlikely	02–Sep–2015
Assets	Inappropriate use of Council assets for private use		8 significant – very likely		6 significant–likely	25–Nov–2015
Petty cash/imprest accounts	Theft of takings disguised by manipulation of accounts		2 minor–unlikely		2 minor–unlikely	25–Nov–2015
Expenses claims	Inflated claims		6 significant–likely		4 significant–unlikely	25–Nov–2015
Corruption	Disposal of assets – land and property		6 serious–unlikely		3 serious–very unlikely	25–Nov–2015
Corruption	Award of planning consents and licences		9 serious–likely		3 serious–very unlikely	25–Nov–2015
Corruption	Acceptance of gifts, hospitality, secondary employment		6 significant–likely		4 significant–unlikely	25–Nov–2015
Car parking	Theft of takings		9 serious–likely		6 serious–unlikely	25–Nov–2015

Page 59

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Treasury management	Falsifying records to gain access to loan or investment monies		12 major – likely		6 serious–unlikely	25–Nov–2015
Money laundering	Using the council to hide improper transactions		8 major – unlikely		4 significant–unlikely	25–Nov–2015
ICT fraud	Improper use of council ICT equipment		12 major – likely		9 serious–likely	25–Nov–2015
Employee – general	Abuse of flexi system Falsification of car loans		6 significant–likely		4 significant–unlikely	25–Nov–2015
Payment of grants to the public	Grants fraudulently claimed		12 major – likely		6 serious–unlikely	25–Nov–2015
Loans & Investments	Misappropriation of funds Fraudulent payment or investment of funds		12 major – likely		4 significant–unlikely	25–Nov–2015
Regeneration development corruption	Regeneration development corruption		12 major – likely		6 serious–unlikely	25–Nov–2015
Financial statements	The financial statements may be materially mis–stated due to fraud		6 serious–unlikely		4 significant–unlikely	25–Nov–2015
New starter	Fraudulent job application		9 serious–likely		4 significant–unlikely	02–Sep–2015
ICT abuse	Improper use of IT equipment		9 serious–likely		4 significant–unlikely	02–Sep–2015
Benefits fraud – internal	Fraudulent claim by member of staff		9 serious–likely		6 serious–unlikely	02–Sep–2015
Cash theft	Theft of takings disguised by manipulation of accounts		4 significant–unlikely		2 significant–very unlikely	25–Nov–2015
Cash theft	Theft of cash without disguise		4 significant–unlikely		1 minor – very unlikely	25–Nov–2015
Payroll	Payment to non existent employees		2 significant–very unlikely		3 serious–very unlikely	25–Nov–2015

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Payroll	Over claiming hours worked		6 significant-likely		2 minor-unlikely	25-Nov-2015
Payroll	Manipulation of standing data		6 serious-unlikely		2 significant-very unlikely	25-Nov-2015
Assets	Theft of current assets		6 significant-likely		4 significant-unlikely	25-Nov-2015
Procurement & Contract Management						
Selection process	Senior staff influencing junior staff involved in a selection process		6 serious-unlikely		4 significant-unlikely	25-Nov-2015
Lack of awareness of the procurement process	Lack of awareness of risks and issues in the procurement process		6 significant-likely		4 significant-unlikely	25-Nov-2015
Lack of anti fraud culture	No antifraud culture – no due diligence/risk registers		6 significant-likely		2 significant-very unlikely	25-Nov-2015
Contract awarded prior to specification being agreed	Contract awarded prior to specifications being fully agreed and developed; meaning the organisation becomes responsible for additional development and training expenses		6 significant-likely		4 significant-unlikely	25-Nov-2015
Manipulation of preferred bidders list	Manipulation of preferred bidders list		4 significant-unlikely		2 significant-very unlikely	25-Nov-2015
No formal contract in place	No formal contract in place		8 significant – very likely		6 significant-likely	25-Nov-2015
Prices reworked	Prices reworked to enable the successful bidder to move up the proposal list following initial bidding		6 significant-likely		4 significant-unlikely	25-Nov-2015

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Value of contract disaggregated	Value of contract disaggregated to circumvent organisation/EU regulations		12 serious – very likely		6 significant–likely	25–Nov–2015
Inappropriate high value purchase	Inappropriate high value purchase for an unauthorised purpose		6 significant–likely		4 significant–unlikely	25–Nov–2015
Inappropriate use of single tender acceptance	Inappropriate use of single tender acceptance		6 significant–likely		4 significant–unlikely	25–Nov–2015
Initial commercial consultations	Procurement staff being sidelined during initial commercial consultations and subsequently being presented with a "done deal".		12 major – likely		6 serious–unlikely	25–Nov–2015
Contract signing	Contracts signed by member of staff not authorised to do so		12 major – likely		6 serious–unlikely	25–Nov–2015
Diversion of funds	Diversion of funds: the risk that a member of staff diverts funds through the set up of non-existent supplier/freelancer		12 major – likely		6 serious–unlikely	25–Nov–2015
Bogus vendor	An individual could authorise the set up of a bogus vendor and raise and authorise a purchase order		16 major – very likely		8 major – unlikely	25–Nov–2015
Sale of confidential information	A member of staff could disclose information on bids to other contract bidders		12 major – likely		6 serious–unlikely	25–Nov–2015
Creditor payments	Fraudulent requests for creditor payments		9 serious–likely		4 significant–unlikely	02–Sep–2015

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Fraudulent use of one off payment	Staff use the cheque payment process to send to a bogus vendor		6 serious–unlikely		2 significant–very unlikely	25–Nov–2015
Declaration of interests	Lack of declarations of interests		9 serious–likely		4 significant–unlikely	25–Nov–2015
Housing tenancy/homelessness						
Housing allocations	Housing allocated for financial reward fraudulent allocation of property		9 serious–likely		4 significant–unlikely	25–Nov–2015
Illegal sub letting	Illegal sub letting of council property		4 significant–unlikely		2 minor–unlikely	25–Nov–2015
Homelessness	False claim of homelessness		6 significant–likely		2 minor–unlikely	25–Nov–2015
Council Tax						
Single Persons Discount	Single persons discount fraudulently claimed		6 significant–likely		6 significant–likely	25–Nov–2015
Discounts/exemptions	Discounts and exemptions falsely claimed		3 minor–likely		2 minor–unlikely	25–Nov–2015
Refund fraud			3 minor–likely		2 minor–unlikely	25–Nov–2015
Suppressed recovery action	Suppressed recovery action		3 minor–likely		2 minor–unlikely	25–Nov–2015
NNDR						
Void exemption	Void exemption falsely claimed		6 significant–likely		4 significant–unlikely	25–Nov–2015
Occupation dates	Occupation dates incorrectly notified		6 significant–likely		4 significant–unlikely	25–Nov–2015
Changes to property	Changes to property increase the rateable value		6 significant–likely		4 significant–unlikely	25–Nov–2015

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Insurance						
Insurance claims	Claiming for non existent injuries Claiming at another establishment for the same injury overclaiming		9 serious–likely		4 significant–unlikely	25–Nov–2015
Other						
Elections	Fraudulent voting Fraudulent acts by canvassers		12 major – likely		6 serious–unlikely	25–Nov–2015
External funding	Fraudulently claiming/using external funding		1 minor – very unlikely		1 minor – very unlikely	25–Nov–2015
Housing Benefits/Council Tax Reduction Scheme						
Benefits fraud – claimant	Claimant fraudulently claims benefits		12 serious – very likely		8 significant – very likely	25–Nov–2015
Benefits fraud – third party eg landlord	fraudulent claim by third party		4 significant–unlikely		4 significant–unlikely	25–Nov–2015
Sheltered schemes	Theft of customer monies		4 significant–unlikely		2 significant–very unlikely	25–Nov–2015






Code of Practice on Managing the Risk of Fraud & Corruption



Report Type: Actions Report
Report Author: Angela Struthers
Generated on: 13 January 2016

Principle Title	Principle Description	Specific Steps	Action to Date	Status	Plan Action Progress to Date
Acknowledge Responsibility	The governing body should acknowledge the responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation.	Acknowledgement – The organisation's leaders acknowledge the threats of fraud and corruption, the harm they can cause and the potential for savings from managing the risks.	The revised policy now includes the sign off acknowledgement		100%
		Culture – The organisation's leaders acknowledge the importance of a culture that is resilient to the threats of fraud and corruption and aligns to the standards of good governance.	The revised policy now includes the sign off acknowledgement		
		Improving resilience – The governing body sets a specific goal for improving its resilience to fraud and corruption	Counter fraud workplan in place and reviewed and reported to the Audit & Governance Committee		
		Responsibility – The governing body acknowledges its responsibility for managing its fraud and corruption risks and will be accountable for the actions it takes through its	This is completed through the reporting of fraud risks to the Audit & Governance Committee		

Page 65

Principle Title	Principle Description	Specific Steps	Action to Date	Status	Plan Action Progress to Date
		governance reports			
Identify Risk	Fraud risk identification is essential to understand specific exposure to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users	Corruption risk – The organisation identifies the risks of corruption in its governance framework	Steps to counter fraud are highlighted in the Annual Governance Statement as part of the governance framework, the counter fraud update is reported to the Audit & Governance Committee		<div style="border: 1px solid black; background-color: #ccccff; padding: 2px; display: inline-block;">66%</div>
		Fraud Risks – Fraud risks are routinely considered as part of the organisation’s strategic risk management arrangements	Fraud risk register is in place and reviewed and reported to the Audit & Governance Committee		
		Measurement of Loss – The organisation uses estimates of fraud loss, and where appropriate measurement exercises, to quantify the harm that different fraud risks cause	Need to establish a measure for fraud loss		
Develop a Strategy	An organisation needs a counter fraud strategy setting out its approach to managing its risk and defining responsibilities for action	Responsibility & Accountability – the strategy includes clear identification of responsibility and accountability for delivery of the strategy and for providing oversight	The Executive Director – Corporate Services has overall responsibility		<div style="border: 1px solid black; background-color: #ccccff; padding: 2px; display: inline-block;">100%</div>
		Strategy – The governing body formally adopts a counter fraud and corruption strategy to address the identified risks and align with the	Included in the statement		

Principle Title	Principle Description	Specific Steps	Action to Date	Status	Plan Action Progress to Date
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Page 67</p>		organisation's acknowledged responsibilities and goals			
		The strategy includes consideration of all the proactive components of a good practice response to fraud risk management:	Developing a counter fraud culture to increase resilience to fraud, deterring fraud attempts by publishing the actions the organisation takes against fraudsters, preventing fraud through the implementation of appropriate and robust internal controls and cyber security measures. All of these areas included in the strategy		
		The strategy includes consideration of all the reactive components of a good practice response to fraud risk management	Detecting fraud through data and intelligence analysis, implementing effective whistleblowing arrangements, investigating fraud referrals, applying sanctions, both civil and criminal, seeking redress, including the recovery of assets and money. All of these areas included in the strategy		
Provide Resources	The organisation should make	Access – The organisation grants	This is stated in Financial		<div style="border: 1px solid black; background-color: #ADD8E6; padding: 2px; display: inline-block;">75%</div>

Principle Title	Principle Description	Specific Steps	Action to Date	Status	Plan Action Progress to Date
Page 68	arrangements for appropriate resources to support the counter fraud strategy	counter fraud staff unhindered access to its employees, information and other resources as required	Guidance		
		Annual assessment – an annual assessment of whether the level of resource invested to counter fraud and corruption is proportionate for the level of risk	Completed as part of the annual review		
		Data sharing – the organisation has protocols in place to facilitate data and intelligence sharing to support counter fraud activity	The Director – Technology & Corporate Programmes has confirmed that the development of the Protocol will be completed by 31 March 2016		
		Skills – the organisation utilises counter fraud staff with appropriate skills and professional accreditation	A Corporate Anti Fraud Investigations Officer has been in post since September 2015 to investigate all fraud		
Take Action	The organisation should put in place the policies and procedures to support the counter fraud and corruption strategy and take action to prevent, detect and investigate fraud	Alignment to Strategy – plans and operations are aligned to the strategy and contributes to the achievement of the organisations overall goal of improving resilience to fraud and corruption	A Counter Fraud Workplan is in place and aligned to the Strategy		
		Annual Report – the governing body receives a report at least annually on the impact and cost effectiveness of	To be completed as part of the annual report to the Audit & Governance		

Principle Title	Principle Description	Specific Steps	Action to Date	Status	Plan Action Progress to Date
		its counter fraud activities	Committee		
		Policy Framework – the organisation has put in place a policy framework which supports the implementation of the counter fraud strategy	The authority has the following policies in place: Counter Fraud & Corruption Strategy, Policy and Guidance Notes Whistleblowing Policy Anti Money Laundering Policy Gifts and Hospitality Policy & Register Codes of Conduct for Members (includes Pecuniary Interests) and staff (includes Declaration of Interests) IT Policies that cover the elements required in a Cyber Security Policy		
		Reporting – there is a report to the governing body at least annually on performance against the counter fraud workplan from the lead person designated in the strategy. Conclusions are featured in the Annual Governance Report	Performance against the Counter Fraud Plan is reported to the Audit & Governance Committee and a statement included in the Annual Governance Statement		

This page is intentionally left blank

AUDIT & GOVERNANCE COMMITTEE

28 JANUARY 2016

REPORT OF THE SOLICITOR TO THE COUNCIL AND MONITORING OFFICER

REGULATION OF INVESTIGATORY POWERS ACT 2000

Purpose

The Council's Code of Practice for carrying out surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) specifies that quarterly reports will be taken to Audit & Governance Committee to demonstrate to elected members that the Council is complying with its own Code of Practice when using RIPA.

Recommendation

That Audit and Governance Committee endorse the quarterly RIPA monitoring report.

Executive Summary

The Office of the Surveillance Commissioner (OSC) conducted an inspection into the RIPA policy, procedures, documentation and training on 6 October 2014 utilised at the Council. The outcome of the inspection was reported to Council on 16 December 2014. The recommendations arising from the inspection have been implemented and reported back to the OSC. The policy at that time was updated in line with the recommendations of the Commissioner and has been published. Training took place on 14 January 2015 for officers who previously had no RIPA training and for members, with refresher training being delivered for those officers previously trained. The feed back from the training has been positive and going forward training for RIPA will be added to the Corporate Training Programme. In May 2015 the RIPA policy was published on Netconsent for all staff with a questionnaire following, this raises awareness of the policy and procedures. The results and feedback from the questionnaire will be used to formulate future training events.

At present the RIPA policy is being reviewed to take account of changes in legislation. The policy shall be submitted for approval and adoption by a separate report however the Council on re-adoption of the RIPA policy shall also be requested to continue with the practice that quarterly reports on the use of RIPA powers be submitted to Audit & Governance Committee.

Options Considered

Obligations arising under RIPA for the authority are statutory therefore the only option is compliance.

Resource Implications

Support for the RIPA obligations and functions are met from existing budget and existing staff resources.

Legal/Statutory and Risk Implications

The recording of applications, authorisations, renewals and cancellations of investigations using covert surveillance techniques or involving the acquisition of communications data is covered by the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act was introduced to regulate existing surveillance and investigation in order to meet the requirements of Article 8 of the Human Rights Act. Article 8 states: Everyone has the right to his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

RIPA investigations can only be authorised by a local authority where it is investigating criminal offences which (1) attract a maximum custodial sentence of six months or more or (2) relate to the sale of alcohol or tobacco products to children.

There are no risk management or Health and Safety implications.

Sustainability Implications

The legislation requires the Authority to record and monitor all RIPA applications, keep the records up to date and report quarterly to a relevant Committee.

Background Information

The RIPA Code of Practice produced by the Home Office in April 2010 introduced the requirement to produce quarterly reports to elected members to demonstrate that the Council is using its RIPA powers appropriately and complying with its own Code of Practice when carrying out covert surveillance. This requirement relates to the use of directed surveillance and covert human intelligence sources (CHIS).

The table below shows the Council's use of directed surveillance in the current financial year to provide an indication of the level of use of covert surveillance at the Council. There have been no applications under RIPA in the period from the date of the last meeting on 24 September 2015 and from 1 October 2015 to 31 December 2015.

The table outlines the number of times RIPA has been used for directed surveillance, the month of use, the service authorising the surveillance and a general description of the reasons for the surveillance. Where an investigation is ongoing at the end of a quarterly period it will not be reported until the authorisation has been cancelled. At the end of the current quarterly period there are no outstanding authorisations.

There have been no authorisations for the use of CHIS.

Financial year 2015/16

Month	Service	Reason
--------------	----------------	---------------

No applications

Background papers

None

"If Members would like further information or clarification prior to the meeting please contact Jane M Hackett Solicitor to the Council and Monitoring Officer on Ext.258"

This page is intentionally left blank

28 JANUARY 2016

REPORT OF THE SOLICITOR TO THE COUNCIL**REGULATION OF INVESTIGATORY POWERS ACT 2000
ADOPTION OF POLICY AND PROCEDURE****EXEMPT INFORMATION**

None

PURPOSE

This report advises Members of the proposed amendments to the Corporate Policy governing the Regulation of Investigatory Powers Act 2000 in light of the new requirements introduced by recent legislative change and Home Office Guidance and seeks their consideration and recommendations in relation thereto.

RECOMMENDATIONS**That the Committee**

- 1. considers the changes to the RIPA policy on Directed Surveillance, Covert Human Intelligence Sources (CHIS) and Acquisition of Communications Data,**
- 2. satisfies itself that the changes meet the requirements imposed on the Council in terms of the legislation and Codes of Practice,**
- 3. provide comments, as required, and**
- 4. recommendation of approval to Cabinet and Council .**

EXECUTIVE SUMMARY

The Council has a number of statutory functions that involve officers investigating the conduct of others with a view to bringing legal action against them. The Council has also been given powers under the Regulation of Investigatory Powers Act 2000 (RIPA) which enable it to carry out Directed Surveillance in certain strict circumstances. RIPA provides a legal framework for the control and regulation of surveillance and information gathering techniques which public bodies such as Tamworth Borough Council have to comply with. These powers have been amended and changed in accordance with various pieces of legislation. The last change resulted in a revised RIPA Policy being approved by the Council in December 2012. The Protection of Freedoms Act 2012 now requires that local authority authorisations under RIPA for Directed Surveillance or CHIS can only become effective on the granting of an order approving the authorisation by a Justice of the Peace. Further a local authority can now only have an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract

a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under the Licensing Act 2003 of the Children and Families Act 2014.

| No Directed Surveillance has been carried out by the Council since 2011 and it is not envisaged that there will be any appreciable change in the foreseeable future. By adhering to this proposed Policy the Council will ensure that the acquisition and disclosure of data is lawful, necessary and proportionate so that the Council is not held to be in breach of Article 8 (the right to respect for private family life, home and correspondence) of the European Convention on Human Rights.

The current policy prepared in 2012 does not reflect recent changes to legislation and Home Office Codes of Practice.

The attached policy and protocol will ensure that the acquisition and disclosure of data is lawful, necessary and proportionate, so that the Council is not held to be in breach of the Human Rights Act and that data obtained under such measures would be used to assist in the successful prosecution of relevant criminal offences.

OPTIONS CONSIDERED

The Policy is to a large extent defined by the requirements of RIPA and the most recent Home Office Codes of Practice. The recommended policy is consistent with the new policies and guidance; there is little scope if any to do otherwise.

RESOURCE IMPLICATIONS

There are no direct resource implications arising from the adoption of the policy and procedure. Any applications and training costs will be met from existing budgets.

LEGAL/RISK IMPLICATIONS

Failure to follow the policy and procedure could result in the Council being open to challenge, unnecessary legal risk and ultimately responsible in damages for any breach of the Codes of Practice and Human Rights legislation. The Office of Surveillance Commissioners would also severely criticise such failure and the adverse publicity arising therefrom could damage the Council's reputation and not serve in its best interests.

The policy and procedure will provide guidance to staff on the processing and procedure to obtain a RIPA authorisation, reducing the risk of legal challenge to the procedure itself and the evidence obtained.

Risk has been identified in the following areas: training of Officers, Collateral Intrusion and changes to legislation and procedures surrounding RIPA, However this has been addressed, regular training of Officers takes place, the Netconsent function and email is used to disseminate the policy and inform training events. The Solicitor to the Council reviews the policy regularly to ensure legislative and Home Office compliance. Quarterly reports are made to Audit & Governance Committee and an annual report to full Council. Finally provision exists in the policy itself to mitigate any other associated risks.

SUSTAINABILITY IMPLICATIONS

Under current arrangements the Policy and training requirements are currently sustainable and remain so for the foreseeable future.

REPORT AUTHOR

Jane Marie Hackett, Solicitor to the Council and Monitoring Officer tel 01827 709258

LIST OF BACKGROUND PAPERS

Regulation of Investigatory Powers Act 2000
Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012
The Protection of Freedoms Act 2012
Home Office – Covert Surveillance and Property Interference Code of Practice
Home Office – Covert Human Intelligence Sources Code of Practice

Appendices

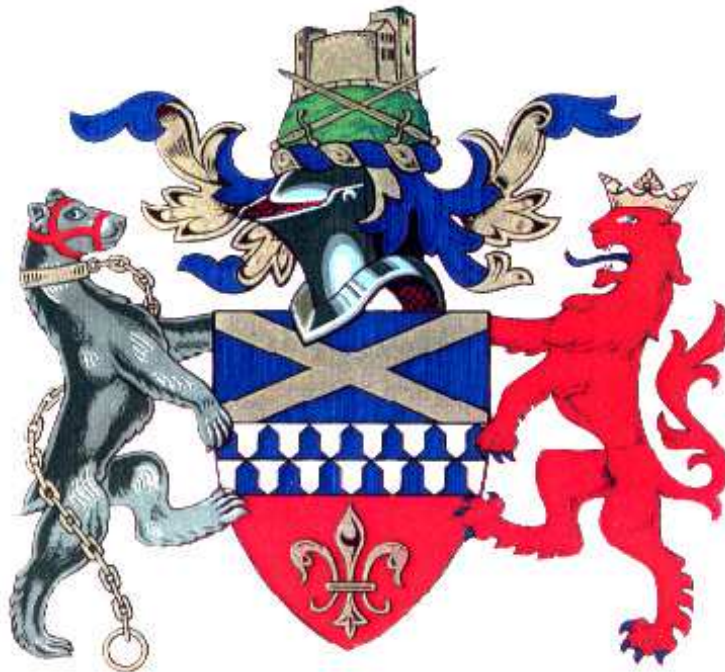
APPENDIX 1 - Proposed RIPA Policy and Procedure

This page is intentionally left blank

TAMWORTH BOROUGH COUNCIL

POLICY & PROCEDURE

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)



Jane Marie Hackett
Solicitor to the Council
Tamworth Borough Council
Policy date: Review: Revised: January 2016

CONTENTS

	Page No.	
Section A	Introduction	3
Section B	Effective Date of Operation and Authorising Officer Responsibilities	5
Section C	General Information on RIPA	7
Section D	What RIPA Does and Does Not Do	8
Section E	Types of Surveillance	9
Section F	Conduct and Use of a Covert Human Intelligence Source (CHIS)	12
Section G	The Role of the RIPA Co-ordinator	18
Section H	Authorisation Procedures	20
Section I	Working with/through other Agencies	29
Section J	Record Management	31
Section K	Acquisition of Communications Data	33
	Conclusion	37
Appendix 1	A Forms – Directed Surveillance	38
Appendix 2	B Forms – CHIS	39
Appendix 3	C Forms – Acquisition of Communications Data	40
Annex A	Local Authority Procedure	41
Annex B	Court Procedure	42
Annex C	Application for Judicial Approval and Order Form	43

Section A

Introduction

1. OBJECTIVE: SUSTAINABLE COMMUNITIES; SAFER AND STRONGER COMMUNITIES

Tamworth Borough Council is committed to improving the quality of life for the communities of Tamworth which includes benefiting from an attractive place to live, meeting the needs of local people and employers with opportunities for all to engage in community life. It also wishes to maintain its position as a low crime borough and a safe place to live, work and learn. Although most of the community comply with the law, it is necessary for Tamworth to carry out enforcement functions to take full action against those who flout the law. Tamworth Borough Council will carry out enforcement action in a fair, practical and consistent manner to help promote a thriving local economy.

2. HUMAN RIGHTS ACT 1998 – ARTICLE 8 – RIGHT TO RESPECT FOR PRIVATE & FAMILY LIFE, HOME AND CORRESPONDENCE

The Human Rights Act 1998 brought into UK domestic law much of the European Convention on Human Rights and Fundamental Freedoms 1950. Article 8 of the European Convention requires the Council to respect the private and family life of its citizens, their homes and their correspondence. Article 8 does, however, recognise that there may be circumstances in a democratic society where it is necessary for the state to interfere with this right.

3. USE OF COVERT SURVEILLANCE TECHNIQUES AND HUMAN INTELLIGENCE SOURCES

The Council has various functions which involve observing or investigating the conduct of others, for example, investigating anti-social behaviour, fly tipping, noise nuisance control, planning (contraventions), benefit fraud, licensing and food safety legislation. In most cases, Council officers carry out these functions openly and in a way which does not interfere with a person's right to a private life. However, there are cases where it is necessary for officers to use covert surveillance techniques to undertake a specific investigation. The use of covert surveillance techniques is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), which seeks to ensure that the public interest and human rights of individuals are appropriately balanced. This document sets out the Council's policy and procedures on the use of covert surveillance techniques and the conduct and use of a Covert Human Intelligence Source. You should also refer to the two Codes of Practice published by the Government. These Codes, which were revised in 2010, are on the Home Office website and supplement the procedures in this document. The Codes are admissible as evidence in Criminal and Civil Proceedings. If a provision of these Codes appear relevant to any court or tribunal, it must be taken into account.

Covert Surveillance and Property Interference Code of Practice:-

<http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-surveil-prop-inter-COP>

Covert Human Intelligence Sources Code of Practice:

<http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-human-intel-source-COP>

There are also two other guidance documents relating the procedural changes regarding the authorisation process requiring Justice of the Peace approval from the 1st November 2012. These have been issued by the Home Office to both Local Authorities and Magistrates.

<http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/>

4. ACQUISITION OF COMMUNICATIONS DATA

RIPA also regulates the acquisition of communications data. Communications data is data held by telecommunications companies and internet service providers. Examples of communications data which may be acquired with authorisation include names, addresses, telephone numbers, internet provider addresses. Communications data surveillance does not monitor the content of telephone calls or emails. This document sets out the procedures for the acquisition of communications data. You should also refer to the Code of Practice which is available on the Home Office website.

Acquisition and Disclosure of Communications Data Revised Draft Code of Practice:

<http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop>

Section B

EFFECTIVE DATE OF OPERATION AND AUTHORISING OFFICER RESPONSIBILITIES

1. The Policy and Procedures in this document have been amended to reflect the two revised Codes of Practice which came into force in April 2010, and the recent legislative amendments which now require Justice of the Peace (JP) approval for all Local Authority RIPA applications and renewals, which came in effect on 1 November 2012, changes in website addresses and application forms, as well as to reflect recommendations arising out of inspection by the Office of Surveillance Commissioners. It is essential, therefore, that Authorising Officers, take personal responsibility for the effective and efficient observance of this document and the Office of Surveillance Commissioners (OSC) guidance documents.
2. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained as 'Applicants'.
3. Authorising Officers will also ensure that staff who report to them follow this Policy and Procedures Document and do not undertake or carry out surveillance activity that meets the criteria as set out by RIPA without first obtaining the relevant authorisations in compliance with this document.
4. Authorising Officers must also pay particular attention to health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until they are satisfied that
 - the health and safety of Council employees/agents are suitably addressed
 - risks minimised so far as is possible, and
 - risks are proportionate to the surveillance being proposed.

If an Authorising Officer is in any doubt, prior guidance should be obtained from the Solicitor to the Council.

5. Authorising Officers must also ensure that, following completion copies of RIPA Forms are immediately sent to the Solicitor to the Council (or any other relevant authority), that they are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'. Any failure to comply exposes the Council to unnecessary legal risk and criticism from the Office of Surveillance Commissioners. Any cancellations must be dealt with in similar manner,
6. In Accordance with the Codes of Practice, the Senior Responsible Officer (SRO) with responsibility for Authorising Officers is the Solicitor to the Council. *The Solicitor to the Council is also the RIPA Co-ordinator. The key responsibilities of the RIPA Co-ordinator are set out in Section G of this document.*

7. The Chief Executive in consultation with Corporate Management Team has power to appoint Authorising Officers for the purposes of RIPA. Authorising Officers will only be appointed on the Chief Executive being satisfied that suitable training on RIPA has been undertaken.
8. The SRO is responsible for
 - the integrity of the process in place within the public authority to authorise directed and intrusive surveillance
 - compliance with Part II of the 2000 Act, and with this code;
 - engagement with the Commissioners and inspectors when they conduct their inspections, and
 - where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.
9. The Solicitor to the Council will review the policy every six months and annual reports on performance of the policy will be presented to Council.
10. Quarterly reports on the use of RIPA will be considered by the Audit and Governance Committee.

Section C

GENERAL INFORMATION ON RIPA

1. The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their homes and their correspondence.
2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-
 - (a) **in accordance with the Law;**
 - (b) **necessary** in the circumstances of the particular case; **and**
 - (c) **proportionate** to what it seeks to achieve.
3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (ie. 'in accordance with the law') for authorising **covert surveillance** and the use of a '**covert human intelligence source**' ('CHIS') – eg. undercover agents. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA and this Policy and Procedure document seeks to ensure both the public interest and the human rights of individuals are suitably balanced.
4. Directly employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf, must be properly authorised by one of the Council's designated Authorising Officers. They may also be inspected by the OSC in respect of that particular operation. This should be pointed out during the instruction and contract stage. It is also important that the Authorising Officer is aware of the abilities of the operatives to ensure they are capable of undertaking the surveillance. Please refer to Section H and to the paragraph on "Authorising Officers."
5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Investigatory Powers Tribunal and the Council could be ordered to pay compensation.

Section D

WHAT RIPA DOES AND DOES NOT DO

1. RIPA:

- requires prior authorisation of directed surveillance.
- prohibits the Council from carrying out intrusive surveillance.
- requires authorisation of the conduct and use of a CHIS.
- requires safeguards for the conduct and use of a CHIS.

2. RIPA does not:

- make lawful conduct which is otherwise unlawful.
- prejudice or affect any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, the Council's current powers to obtain information from the DVLA or from the Land Registry as to the ownership of a property.

3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Solicitor to the Council BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

Section E

TYPES OF SURVEILLANCE

'Surveillance' includes:

- monitoring, observing and listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It may be conducted with or without the assistance of a surveillance device.
- recording anything mentioned above in the course of authorised surveillance.
- surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. They will be going about Council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (eg. where a noisemaker is warned (preferably in writing) that noise will be recorded).

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA).

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

Directed Surveillance

Directed Surveillance is surveillance which:-

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

Private Information in relation to a person includes any information relating to his private and family life, his home or his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others with whom s/he comes into contact. Private information may include personal data such as names, addresses or telephone numbers. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. Privacy considerations are likely to arise if several records are examined together to establish a pattern of behaviour.

For the avoidance of doubt, only those Officers appointed as ‘Authorising Officers’ for the purpose of RIPA can authorise ‘Directed Surveillance’ IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, are followed.

Intrusive Surveillance

This is when it:-

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

This form of surveillance can be carried out only by police and other law enforcement agencies. Intrusive surveillance relates to the location of the surveillance, and not any consideration of the information that is likely to be obtained. Council officers cannot carry out intrusive surveillance.

“Necessity”

The covert surveillance activity must be necessary in the circumstances of the particular case. The surveillance has to be necessary and required to achieve the aims of the investigation and it must fulfil the criteria required in law relating to a criminal offence or offences that are either punishable, whether on summary conviction or indictment by a maximum term of at six months imprisonment or more, or are related to the underage sale of alcohol and tobacco. The application must

explain in detail why it is necessary to use covert surveillance to achieve this aim for example why is it not possible to obtain the information from another source.

“Proportionality”

This term contains three concepts:-

- the surveillance should not be excessive in relation to the gravity of the matter being investigated;
- the least intrusive method of surveillance should be chosen; and
- collateral intrusion involving invasion of third parties' privacy and should, so far as possible, be minimised.

Proportionality involves balancing the intrusiveness of the activity on the subject and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case, or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.

The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.

The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers :

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

When considering the intrusion, it is important that the Authorising Officer is fully aware of the technical capabilities of any proposed equipment to be used, and that any images are managed in line with the Data Protection Act and Home Office Guidance. These issues have a direct bearing on determining proportionality.

Section F

Covert Human Intelligence Source (CHIS)

Staff will need to know when someone providing information may become a CHIS, and in these circumstances the Council is required to have procedures in place should this be necessary. However If it appears that use of a CHIS may be required, Authorising Officers must seek legal advice from the Solicitor to the Council.

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However, the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources.

Under section 26(8) of the 2000 Act a person is a 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 to 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.

By virtue of section 26(9)(b) of the 2000 Act 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 the purpose.

By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above 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.

An example would be where a Council member of staff uses social media sites to obtain information on a person's activities. If the member of staff became a "friend" using a pseudo account to conceal their identity intending to obtain private information this is covert activity, and as such will require an authorisation for directed surveillance. However there is also the possibility that the member of staff is engaged in intrusive surveillance if the social media site connects to a room in a person's private dwelling. In addition should the member of staff engage in any form of relationship with the person s/he is likely to become a CHIS, authorisation is required and management by a Controller and Handler, records need to be kept and a risk assessment completed, care has to be taken to avoid such status drift.

Conduct and Use of a Source

The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

The **conduct of a source** is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfill whatever tasks are given to them or which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

When completing applications for the use of a CHIS, the applicant must state who the CHIS is, what they can do and for which purpose.

When determining whether a CHIS authorisation is required, consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

Management of Sources

Within the provisions there has to be;

- (a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare (**Handler**)
- (b) at all times there will be another person who will have general oversight of the use made of the source (**Controller**)
- (c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

The **Handler** will have day to day responsibility for:

- dealing with the source on behalf of the authority concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare;

The **Controller** will be responsible for the general oversight of the use of the source.

Tasking

Tasking is the assignment given to the source by the Handler or Controller by asking him to obtain information, to provide access to information, or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice

Management Responsibility

The Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary, the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

Security and Welfare

The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

Record Management for CHIS

Proper records must be kept of the authorisation and use of a source. The particulars to be contained within the records are;

- a. the identity of the source;
- b. the identity, where known, used by the source;
- c. any relevant investigating authority other than the authority maintaining the records;
- d. the means by which the source is referred to within each relevant investigating authority;
- e. any other significant information connected with the security and welfare of the source;
- f. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- g. the date when, and the circumstances in which the source was recruited;
- h. the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- i. the periods during which those persons have discharged those responsibilities;
- j. the tasks given to the source and the demands made of him in relation to his activities as a source;
- k. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- l. the information obtained by each relevant investigating authority by the conduct or use of the source;
- m. any dissemination by that authority of information obtained in that way; and
- n. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. those under the age of 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person with parental responsibility for him or her. Only the Chief Executive, or in his absence, the Deputy Chief Executive can authorise the use of a juvenile as a source.

Vulnerable Individuals

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive, or in his absence, the Deputy Chief Executive can authorise the use of a vulnerable individual as a source.

Test Purchases

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

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance. However it will be necessary to complete the relevant separate application forms.

Authorising Officers should consider the likelihood that the test purchase will lead to a relationship being formed with a person in the shop. If the particular circumstances of a particular test purchase are likely to involve the development of a relationship Authorising Officers must seek legal advice from the Solicitor to the Council.

If several shop premises are included on one application for Directed Surveillance, each premises will be required to be assessed by the Authorising Officer individually on their own merits.

Anti-Social Behaviour Activities (eg. Noise, Violence, Race etc)

As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour, unless there are

criminal offences involved which attract a maximum custodial sentence of six months. Should it be necessary to conduct covert surveillance for disorder which does not meet the serious crime criteria of a custodial sentence of a maximum of six months, this surveillance would be classed as surveillance outside of RIPA, and would still have to meet the Human Rights Act provisions of Necessity and Proportionality? (See section of surveillance outside of RIPA)

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

DRAFT

Section G

THE ROLE OF THE RIPA CO-ORDINATOR

Key Responsibilities of the RIPA Co-ordinator

In this document the RIPA Co-ordinator is the Solicitor to the Council. The key responsibilities of the RIPA Co-ordinator are to:

- Retain all applications for authorisation (including those that have been refused), renewals and cancellations for a period of at least **three years** together with any supplementary documentation;
- Provide a unique reference number and maintain the central register of all applications for authorisations whether finally granted or refused (see section below);
- Create and maintain a spreadsheet for the purpose of identifying and monitoring expiry dates and renewal dates although the responsibility for this is primarily that of the officer in charge and the Authorising Officer;
- Retain and maintain an oversight of the authorisation process
- Monitor types of activities being authorised to ensure consistency and quality throughout the Council;
- Ensure sections identify and fulfil training needs;
- Periodically review Council procedures to ensure that they are up to date;
- Assist Council employees to keep abreast of RIPA developments by organising training and raising RIPA awareness throughout the Council;
- Provide a link to the Surveillance Commissioner and disseminate information on changes on the law, good practice etc. Officers becoming aware of such information should, conversely, send it to the RIPA Co-ordinator for this purpose;
- Check that Authorising Officers carry out reviews and cancellations on a timely basis.

Central Record of Authorisations

A centrally retrievable record of all authorisations will be held by the RIPA Co-ordinator (Solicitor to the Council) which must be up-dated whenever an authorisation is granted, renewed or cancelled. These records will be retained for a period of **three years** from the ending of the authorisation and will contain the following information:

- The type of authorisation;
- The date the authorisation was given;
- The name and title of the Authorising Officer;
- The unique reference number of the investigation (URN);
- The title of the investigation or operation, including a brief description and the names of the subjects, if known;
- Whether the investigation will obtain confidential information;
- Whether the authorisation was granted by an individual directly involved in the investigation;
- The date approved by the Magistrate
- The dates the authorisation is reviewed and the name and title of the Authorising Officer;
- If the authorisation is renewed, when it was renewed and the name and title of the Authorising Officer;
- The date the authorisation was cancelled.
- Joint surveillance activity where Council staff have been authorised on another agencies authorisation will also be recorded.

Access to the data will be restricted to the RIPA Co-ordinator and Authorising Officers to maintain the confidentiality of the information.

Section H

AUTHORISATION PROCEDURES

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

Authorising Officers

Forms can only be signed by Authorising Officers. The Authorising Officers are:

Chief Executive	Tony Goodwin
Executive Director Corporate Services	John Wheatley
Director Assets & Environment	Andrew Barratt

Appointment of the aforesaid officers is subject to the training requirements set out in the paragraph below.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and any internal departmental Schemes of Management.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time.**

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises such an investigation or operation the centrally retrievable record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during the next inspection.

Training

Authorising Officers will only be appointed if the Chief Executive is satisfied that they have undertaken suitable training on RIPA. Evidence of suitable training is to be supplied in the form of a certificate/confirmation from the trainer to the effect that the Authorising Officer has completed a suitable course of instruction.

The Solicitor to the Council will maintain a Register of Authorising Officers and details of training undertaken by them.

If the Chief Executive is of the view that an Authorising Officer has not complied fully with the requirements of this document, or the training requirements then that Officer's authorisation can be withdrawn until they have undertaken further approved training or has attended a one-to-one meeting with the Chief Executive.

Grounds for Authorisation

On 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace:** The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**
- **Directed surveillance crime threshold:** The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (“the 2012 Order”) states that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating (1) criminal offences which attract a maximum custodial sentence of six months or more or (2) criminal offences under sections 146, 147 or 147A of the Licensing Act 2003 or sections 91 and 92 of the Children and Families Act 2014 relating to the sale of alcohol and/or tobacco products to children.

The crime threshold, as mentioned is only for Directed Surveillance.

Therefore the only lawful reason is **prevention and detection of crime** in respect of its Core Functions. As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour unless there are criminal offences involved which attract a maximum custodial sentence of six months or more.

APPLICATION PROCESS

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP’s approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP’s approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete

the required section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing. The hearing will be in private and heard by a single JP.

The Authorising Officer will be expected to attend the hearing along with the applicant officer. Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the Solicitor to the Council.

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case, and the original application/authorisation form.

The original RIPA application/authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA application/ authorisation and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. **However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.**

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to

Approve the Grant or renewal of an authorisation

The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case. The duration of the authorisation commences with the magistrate's approval.

Refuse to approve the grant or renewal of an authorisation

The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the application/authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the application/authorisation or renew the application/authorisation and decides to quash the original authorisation or notice. However the court must not exercise its power to quash the application/authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the Legal section who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA application and authorisation form and the judicial application/order form. The officer will retain the original application/authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, The officers are now allowed to undertake the activity.

The original application and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and if necessary by the Authorising Officer.

A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal team will decide what action if any should be taken.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

An application for an authorisation must 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 directed surveillance or the use of a CHIS.

Application, Review, Renewal and Cancellation Forms

Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. Applications whether authorised or refused will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations.

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP's approval. The duration of the authorisation commences with the magistrate's approval. (see procedure above RIPA application and authorisation process)

Duration of Applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Juvenile Sources	1 Month
Renewal	12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire. (See cancellations page 16)

Reviews

The reviews are dealt with internally by submitting the review form to the authorising officer. There is no requirement for a review form to be submitted to a JP. However if a different surveillance techniques is required is is likely a new application will have to be completed and approved by a JP.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

Renewal

Should it be necessary to renew a Directed Surveillance or CHIS application/authorisation, this must be approved by a JP.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusion issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and

information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the authorising officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraph 5.18 in the Codes of Practice). **It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the Senior Responsible Officer.**

The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Before an Authorising Officer signs a Form, they must:-

- (a) Be mindful of this Policy & Procedures Document and the training undertaken
- (b) Be satisfied that the RIPA authorisation is:-
 - (i) **in accordance with the law and**
 - (ii) **necessary** in the circumstances of the particular case on the ground mentioned (see section on necessity at page 10) **and**
 - (iii) **proportionate** to what it seeks to achieve by acquiring such data. (see section on proportionality at page 11)
- (c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information.

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 fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidence, what other methods have been considered and why they were not implemented.

The least intrusive method will be considered proportionate by the courts.

- (d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**collateral intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion. This matter may be an aspect of determining proportionality;
- (e) Set a date for review of the authorisation and review on only that date;
- (f) Obtain a Unique Reference Number (URN) for the application from the Solicitor to the Council on 01827 709258

- (g) Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Solicitor to the Council, Central Register, **within 5 working days of the relevant authorisation, review, renewal, cancellation or rejection.**

Additional Safeguards when Authorising a CHIS

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

- (a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved.
- (b) Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;
- (c) Consider the likely degree of intrusion of all those potentially affected;
- (d) Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;
- (e) Ensure **records** contain particulars and are not available except on a need to know basis.
- (f) Ensure that if the CHIS is under the age of 18 or is a vulnerable adult the Authorising Officer is the Chief Executive or in his absence, the Deputy Chief Executive.

The Authorising Officer must attend to the requirement of section 29(5) RIPA and of the Regulation of Investigatory Powers (Source Records) Regulations 2000. It is strongly recommended that legal advice is obtained in relation to the authorisation of a CHIS.

Urgent Authorisations

As from 1 November 2012 there is no longer provision under RIPA for urgent oral authorisations.

Section I

WORKING WITH / THROUGH OTHER AGENCIES

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. The agency must be made aware explicitly what they are authorised to do. The agency will be provided with a copy of the application form (redacted if necessary) or at the least the authorisation page containing the unique number.

Equally, if Council staff are authorised on another agencies RIPA authorisation, the staff will obtain a copy of the application form (redacted if necessary), or at the least the authorisation page containing the unique number, a copy of which should be forwarded for filing within the central register. They must ensure that they do not conduct activity outside of that authorisation.

Provisions should also be made regarding any disclosure implications under the Criminal Procedures Act (CPIA) and the management, storage and dissemination of any product obtained.

When another agency (e.g. Police, Customs & Excise, Inland Revenue etc):-

- (a) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, the Officer must obtain a copy of that agency's RIPA form (redacted if necessary) or at the least the authorisation page containing the unique number for the record (a copy of which must be passed to the Solicitor to the Council for the Central Register) Should this be an urgent oral authorisation they should obtain a copy of the contemporaneous notes of what has been authorised by the Authorising Officer in line with current guidance. A copy of these notes will be forwarded for filing in the central register.
- (b) wish to use the Council's premises for their own RIPA action, the Chief Officer or Head of Service should, normally, cooperate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's cooperation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

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

Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation is to take place.

If in doubt, please consult with the Solicitor to the Council at the earliest opportunity.

DRAFT

Section J

RECORD MANAGEMENT

The Council must keep detailed records of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Solicitor to the Council.

Records Maintained in the Department

The following documents must be retained by the Department authorising the surveillance:

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

Central Register maintained by the Solicitor to the Council

Authorising Officers must forward a copy of the form to the Solicitor to the Council for the Central Register, within 5 working days of the authorisation, review, renewal, cancellation or rejection. The Solicitor to the Council will monitor the same and give appropriate guidance to Authorising Officers from time to time, or amend this document in the light of changes of legislation or developments through case law.

Retention and Destruction of Material

Arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. Authorising Officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorised relating to the handling and storage of material.

The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

The Office of the Surveillance Commissioners will also write to the Council from time to time, requesting information as to the numbers of authorisations made in a specific period. It will be the responsibility of the Solicitor to the Council to respond to such communications.

Errors

There is now a requirement as set out in the OSC procedures and Guidance 2011 to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This would be known as an error. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Council's RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. (See oversight section below)

Section K

ACQUISITION OF COMMUNICATIONS DATA

What is Communications Data?

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

Powers

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies (“Communications Companies”).

S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a private telecommunications company is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves.

In order to compel a communications company to obtain and disclose, or just disclose communications data in their possession, a notice under S22 (4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a permitted Local Authority is for the purposes of “preventing or detecting crime or of preventing disorder”. The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Company will most probably have means of collating and providing the communications data requested.

Single Point of Contact

To obtain communication data the request must be submitted through a “Single Point of Contact” (“SPoC”). The National Anti-Fraud Network (NAFN) have been given the responsibility to act as the SPoC for all local authorities. **No Council can obtain communications data through RIPA without using NAFN.**

The role of the SPoC is to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data. All SPoC officers are registered with the Home Office.

The functions of the SPoC are to:

- Assess, where appropriate, whether access to communications data is reasonably practical for the postal or telecommunications operator;

- Advise Applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators
- Advise Applicants and Authorising Officers on whether communications data falls under section 21(4)(a), (b) or (c) of RIPA
- Provide safeguards for authentication
- Assess any cost and resource implications to both the Council and postal or telecommunications operator.

The Senior Responsible Officer

In accordance with the Code of Practice each public authority must have a Senior Responsible Officer who is responsible for:

- The integrity of the process in places within the public authority to acquire communications data;
- Compliance with Chapter II of Part 1 of RIPA and with the Code;
- Oversight of the reporting of errors to the Interception of Communications Commissioner's Office (IOCCO) and the identification of both the cause of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the IOCCO inspectors when they conduct their inspections and;
- Where necessary, oversee the implementation of post – inspection action plans approved by the Commissioner

The Council's Senior Responsible Officer is the Solicitor to the Council.

Application Forms

Only the approved Accessing Communications Data forms referred to in Appendix 4 must be used. The forms have to be downloaded and completed in the Applicants handwriting

Procedure

All applications to obtain communications data must be channelled through the NAFN as the SPoC. The application process is conducted online using their system. If an investigating officer is considering making an application to obtain communications data they should contact the SPoC for advice and to complete the application process.

In completing the online forms the investigating officer must address the issues of necessity, proportionality and collateral intrusion. The following is guidance on the principles of necessity, proportionality and collateral intrusion.

“Necessity” should be a short explanation of the crime (together with details of the relevant legislation), the suspect, victim or witness and the telephone or communications address and how all these three link together. It may be helpful to outline the brief details of the investigation and the circumstances leading to the application as this will assist with justifying necessity. The source of the telephone

number or communications address should also be outlined. E.g. if the number was obtained from itemised billing or a business flyer there should be specific identifiers such as the telephone number or exhibit number.

“Proportionality” should be an outline of what the investigating officer expects to achieve from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. The investigating officer should give an explanation as to why specific date/time periods of data have been requested. An explanation of what is going to be done with the communications data once it is acquired and how that action will benefit the investigation will assist with the justification of proportionality. The investigating officer should outline what other checks or methods have been tried e.g. visiting other known addresses, ringing the number etc or why such methods are not deemed feasible.

“Collateral intrusion” should also be addressed on the suspect or individual in question to demonstrate that the intrusion is not arbitrary or unfair. It is regarded that there will be no collateral intrusion in relation to subscriber checks as no matter who the number is registered to they will form some part of investigative enquiries. In some case it will be clear that the suspect has been contacted on the actual telephone number by the complainant or the investigating officer and therefore this reduces the potential for collateral intrusion. Investigating officers should also mention whether it is known that the telephone number (or other type of data) has been used for example to advertise the business, either in the press/internet or on business cards/flyers as this would also be evidence to show that the suspect is actually using the telephone number and further reduce the potential for collateral intrusion. Collateral intrusion becomes more relevant when applying for service use data such as itemised billing and investigating officers should outline specifically what collateral intrusion may occur, how the time periods requested impact on collateral intrusion and whether they are likely to obtain data which is outside the realm of their investigation.

Once the investigating officer has completed the online application form it is automatically forwarded to the SPoC. If the SPoC is satisfied that the application should proceed, the Application and the draft Notice to the Communications Service Provider will be electronically forwarded for consideration by an Authorising Officer¹. If the SPoC decides that the application is not justified it will be rejected. If the SPoC requires further information, in order to consider the application this will be requested from the investigating officer.

The Authorising Officer must consider:

- (a) whether the case justifies the accessing of communications data for the **purposes of preventing or detecting crime or of preventing disorder** and why obtaining the data is **necessary** in order to achieve the aims of the investigation and on the grounds permitted to the Council;

and

- (b) whether obtaining access to the data by the conduct authorised, or required of the postal or telecommunications operator in the case of a notice, is **proportionate** to what is sought to be achieved.

The Authorising Officer will complete the online application form as appropriate.

If the Authorising Officer becomes directly involved in the operation, such involvement and their justification for undertaking the role of Authorising Officer must be explicit in the written considerations on the Application Form or alternatively the application should be passed to another Authorising Officer for consideration.

If the accessing of communications data is authorised by the Authorising Officer it will also need approval by a Magistrate. The online forms will be completed so that NAFN can acquire the data should it be approved.

1. NOTE: The Code of Practice referred to in paragraph 5 above refers to "Designated Persons" as those whose authority is obtained with regard to the application. However, for the purposes of this policy and procedure the term "Authorising Officer" will be used for that of "Designated Person".

Duration

Authorisations and notices are only valid for one month. A shorter period should be specified if this is satisfied by the request. An authorisation or notice may be renewed during the month by following the same procedure as obtaining a fresh authorisation or notice.

An Authorising Officer shall cancel an authorisation or notice as soon as it is no longer necessary or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the Authorising Officer who issued it.

Record Management

Applications, authorisations and notices for communications data must be retained by the SPoC until audited by the IOCCO. All such documentation must be kept in locked storage.

Errors

Where any errors have occurred in the granting of authorisations or the giving of notices, a record shall be kept and a report and explanation sent to the IOCCO as soon as reasonably practicable.

Oversight

The IOCCO will write to the Council from time to time requesting information as to the numbers of applications for communications data and confirmation as to whether there have been any errors which have occurred when obtaining data communications. It will be the responsibility of the Solicitor to the Council to respond to such communications.

Section L

CONCLUSION

Obtaining an authorisation under RIPA and following the guidance and procedures in this document will assist in ensuring that the use of covert surveillance or a CHIS is carried out in accordance with the law and subject to safeguards against infringing an individual's human rights. Complying with the provisions of RIPA protects the Council against challenges for breaches of Article 8 of the European Convention on Human Rights.

Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign or rubber stamp Form(s) without thinking about their personal and the Council's responsibilities.

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

For further advice and assistance on RIPA, please contact the Solicitor to the Council (who is also the Monitoring Officer).

APPENDIX 1

A FORMS

DIRECTED SURVEILLANCE

All forms can be obtained from:

<http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/>

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Application for Authorisation Directed Surveillance

Application for Review of a Directed Surveillance Authorisation

Application for Renewal of a Directed Surveillance Authorisation

Application for Cancellation of a Directed Surveillance Authorisation

APPENDIX 2

B FORMS

CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

All forms can be obtained from:

<http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/>

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Application for Authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS).

Application for Review of a Covert Human Intelligence Source (CHIS) Authorisation.

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation.

Application for Cancellation of an authorisation for the use or Conduct of a Covert Human Intelligence Source.

APPENDIX 3

C FORMS

ACQUISITION OF COMMUNICATIONS DATA

All forms can be obtained from the Home Office: RIPA Codes of Conduct website:
<http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/>

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Part I Chapter II request schedule for subscriber information

Specimen Part I Chapter II authorisation

Specimen Part I Chapter II Notice

Chapter II application for communications data

Guidance notes regarding chapter II application form

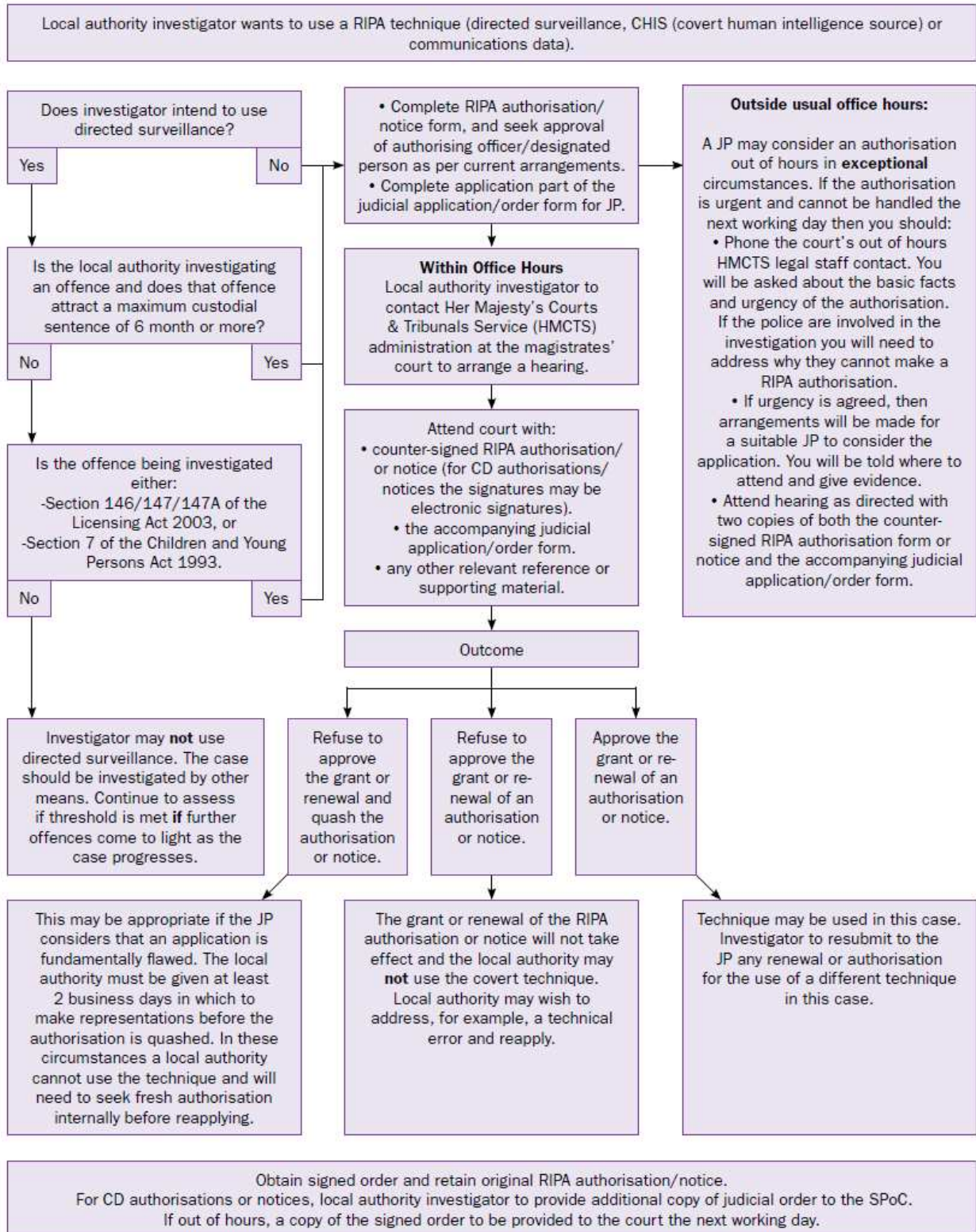
RIPA Section 22 notice to obtain communications data from communications service providers

Reporting an error by a CSP to the IOCCO

Reporting an error by a public authority to the IOCCO

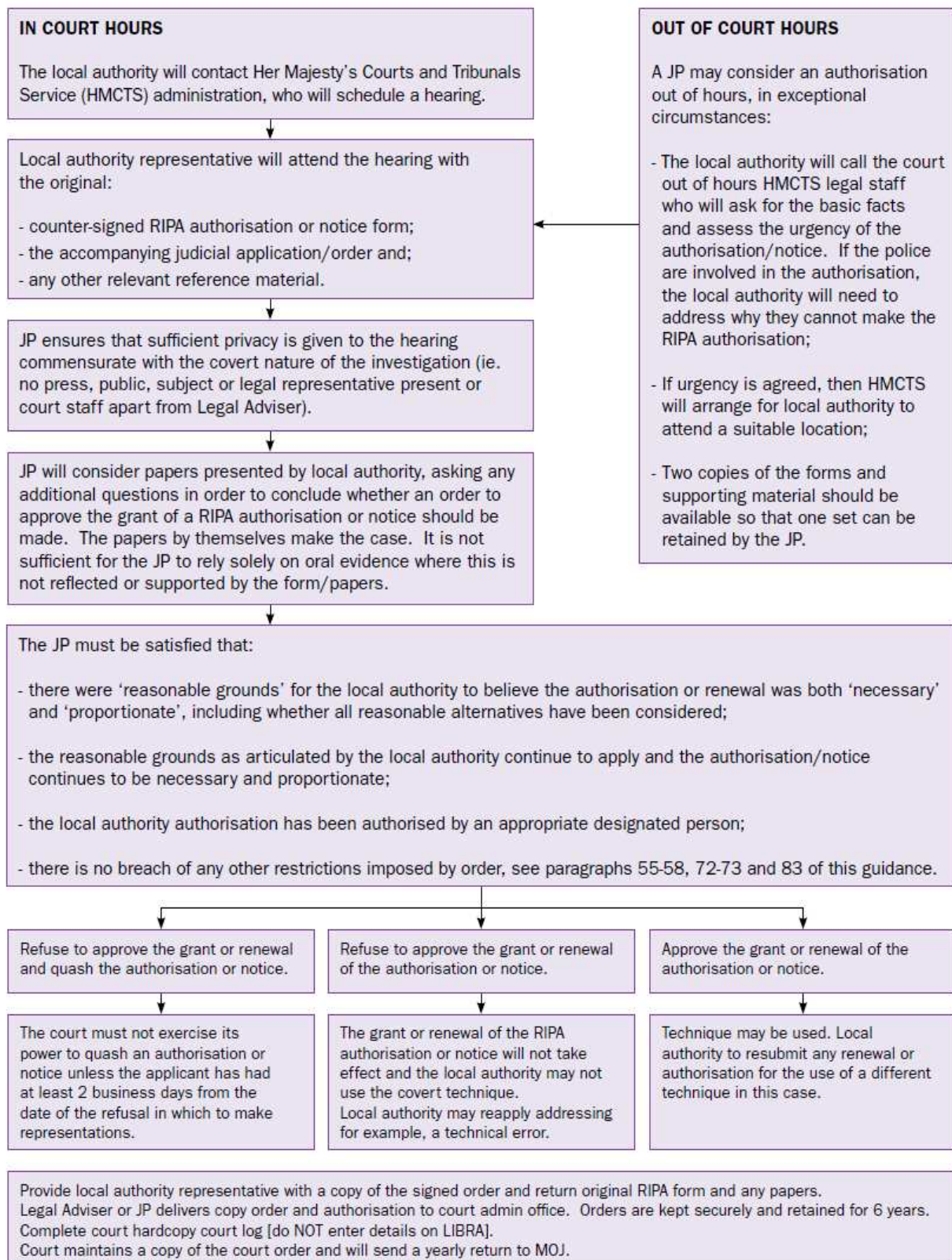
Annex A Local Authority Procedure

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Annex B Court Procedure

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local thorty:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data

Covert Human Intelligence Source

Directed Surveillance

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

- am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal of the authorisation/notice.
- refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....
.....
.....
.....
.....

Reasons

.....
.....
.....
.....
.....
.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

AUDIT & GOVERNANCE COMMITTEE

28 JANUARY 2016

Report of Solicitor to the Council and Monitoring Officer

STANDARDS ALLEGATION COMPLAINTS

Purpose

To advise Members in relation to recent complaints received which alleged that a breach of the Code of Conduct occurred under the local arrangements that were put in place to deal with Standards allegations, in terms of the Localism Act 2011, by Council on 19 June 2012.

Recommendation

Members are requested to endorse the findings of the contents of the report.

Executive Summary

In the year to 31 December 2015 two complaints were lodged.

The first complaint was received following Cabinet on 10 September 2015.-
Complaint One.

Complaint One, was made by one member against another member. In terms of the Policy for dealing with complaints of this nature the Monitoring Officer invoked the procedure to resolve the issue without resorting to the complaints process. Informal contact was made with the member against whom the complaint had been lodged. A resolution was proposed and invoked accordingly. The action taken is in accordance with the Arrangements for Dealing with Standards Allegations under the Localism Act 2011 that were adopted at Council on 19 June 2012

Complaint One was dealt with as follows:

On 1 October 2015 the member delivered a full apology for his actions at Cabinet which was accepted by the complainant.

The second complaint was received at Council on 15 September 2015.-
Complaint Two.

Complaint Two, was made by a member who moved a motion without notice at the Council meeting on 15 September 2015 which comprised a complaint against another member. In terms of the Policy for dealing with complaints of this nature the Monitoring Officer invoked the procedure to

resolve the issue without resorting to the complaints process. Informal contact was made with the member against whom the complaint had been lodged. A resolution was proposed and invoked accordingly. The action taken is in accordance with the Arrangements for Dealing with Standards Allegations under the Localism Act 2011 that were adopted at Council on 19 June 2012

Complaint Two was dealt with as follows:

On 15 December 2015 the member delivered an apology for his actions at Council which was accepted by the complainant.

Options Considered

The procedure for dealing with complaints against a Councillor for an alleged breach of the Code of Conduct requires the Monitoring Officer to report Informal Resolutions to the Audit and Governance Committee for information.

Resource Implications

As the matter has been resolved using the informal resolution process the resources utilised have been totally contained within the corporate core cost centre.

Legal/Risk Implications

Without a process to deal with complaints of this nature against members the authority would be operating ultra vires and risk legal action and/or damage to reputation. The cost in financial terms could be significant.

Sustainability Implications

The process and policy for dealing with complaints of this nature provides as robust a system as possible in the current legislative climate. The process and policy is kept under review and amended in line with Council protocols.

Background Information

Since the establishment of the new arrangements from June 2012 I can confirm that the system adopted in relation to Standards allegations has operated satisfactorily and high standards of conduct are being maintained in the authority. The legislation does not give the Council any powers to impose sanctions, such as suspension or requirements for training or an apology, on members in relation to a breach of conduct. Accordingly, where a failure to comply with the Code of Conduct is found, the range of sanctions which the authority can take in respect of the member is limited and must be directed to

securing the continuing ability of the authority to systematically discharge its functions effectively, rather than “punishing” the member concerned.

Report Author

Jane M Hackett, Solicitor to the Council & Monitoring Officer (Extn: 258)

List of Background Papers

Localism Act 2011

Report to Council dated 19 June 2012 – Changes to the Standards Regime Procedure and Process for dealing with and making a complaint against a Councillor for an Alleged Breach of the Code of Conduct.

This page is intentionally left blank

Planned Reports to Audit & Governance Committee (Draft)

	Report	Committee Date	Report of	Comments
1	Internal Audit annual & quarterly update	June	Head of Internal Audit	
2	Risk Management quarterly update	June	Head of Internal Audit	
3	Review of the effectiveness of Internal Control Environment	June	Head of Internal Audit	To include the review of the effectiveness of internal audit, compliance with PSIAS, roles of the CFO and HIAS
4	Counter Fraud update	June	Head of Internal Audit	
5	Role of the Audit Committee	June	Grant Thornton	Presentation/training
1	Draft Annual Statement of Accounts	June	Executive Director Corporate Services	
2	Annual Governance Statement & Code of Corporate Governance	June	Head of Internal Audit	
3	Review of the Constitution & Scheme of Delegation for Officers	June	Solicitor to the Council and Monitoring Officer	
4	Audit & Governance Committee Update	June	Grant Thornton	
5	Fee Letter	June	Grant Thornton	
6	RIPA Quarterly Report	June	Solicitor to the Council and Monitoring Officer	

	Report	Committee Date	Report of	Comments
1	Annual Statement of Accounts	September	Executive Director Corporate Services	
2	Audit Findings Report	September	Grant Thornton	
3	Internal Audit quarterly update	September	Head of Internal Audit	
4	Risk Management quarterly update	September	Head of Internal Audit	
6	Treasury Management Strategy Statement and Annual Investment Strategy Mid-year Review Report 2013/14	September	Executive Director Corporate Services	
7	RIPA Quarterly Report	September	Solicitor to the Council and Monitoring Officer	
8	Local Government Ombudsman's Annual Review and Report 2013/14	September	Solicitor to the Council and Monitoring Officer	
1	Annual Audit Letter 2013/14	October	Grant Thornton	
2	Internal Audit quarterly update	October	Head of Internal Audit	
3	Risk Management quarterly update	October	Head of Internal Audit	
4	Annual Governance Statement update	October	Head of Internal Audit	

	Report	Committee Date	Report of	Comments
5	Members/Standards	October	Solicitor to the Council & Monitoring Officer	
6	Anti Money Laundering Policy	October	Solicitor to the Council & Monitoring Officer	
1	Audit Report on Certification Work 2013/14	January	Grant Thornton	
2	Audit Progress Report	January	Grant Thornton	
3	Internal Audit quarterly update	January	Head of Internal Audit	
4	Risk Management quarterly update	January	Head of Internal Audit	
5	Counter Fraud update	January	Head of Internal Audit	To include review of Counter Fraud Policy and Whistleblowing Policy
6	Review of Financial Guidance	January	Head of Internal Audit	
7	RIPA Quarterly Report	January	Solicitor to the Council and Monitoring Officer	
8	Treasury Management mid year monitoring report	January	Executive Director Corporate Services	
1	Final Accounts 2014/15 – Action Plan	March	Director of Finance	
2	Draft Audit Plan	March	Grant Thornton	
3	Draft Certification Work Plan	March	Grant Thornton	

	Report	Committee Date	Report of	Comments
4	Audit Committee Update	March	Grant Thornton	
5	Auditing Standards	March	Grant Thornton	
6	Internal Audit Charter and Audit Plan	March	Head of Internal Audit	
7	Audit & Governance Committee Self Assessment	March	Head of Internal Audit	
8	RIPA Quarterly Report	March	Solicitor to the Council and Monitoring Officer	
9	Treasury Management Strategy and Prudential Indicators	March	Executive Director Corporate Services	

Portfolio Holder CS - Portfolio Holder for Corporate Services & Assets