



Borough of Tamworth

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

Enquiries: 01827 709 709
Facsimile: 01827 709 271

AUDIT AND GOVERNANCE COMMITTEE

18 October 2017

Dear Councillor

A meeting of the Audit and Governance Committee will be held in **Committee Room 1 - Marmion House on Thursday, 26th October, 2017 at 6.00 pm.** Members of the Committee are requested to attend.

Yours faithfully

A handwritten signature in black ink, consisting of a stylized 'A' followed by a long horizontal line that tapers to a point.

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** (Pages 5 - 18)
(Report of Grant Thornton – External Auditor)
- 5 Audit and Governance Committee Update - Progress Report and Update**
(Pages 19 - 36)
(Report of Grant Thornton – External Auditor)
- 6 Local Government Ombudsman Annual Review 2016/17** (Pages 37 - 50)
(Report of the Solicitor to the Council and Monitoring Officer)
- 7 Regulation of Investigatory Powers Act 2000** (Pages 51 - 106)
(Report of the Solicitor to the Council and Monitoring Officer)
- 8 Internal Audit Update Report 2017/18** (Pages 107 - 128)
(Report of the Head of Internal Audit Services)
- 9 Risk Management Update** (Pages 129 - 142)
(Report of the Head of Internal Audit Services)
- 10 Counter Fraud Update** (Pages 143 - 204)
(Report of the Head of Internal Audit Services)
- 11 Audit and Governance Committee Timetable** (Pages 205 - 208)
(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: M Summers, R Ford, C Cooke, J Faulkner, M Gant, M Greatorax and
R Kingstone

This page is intentionally left blank



MINUTES OF A MEETING OF THE AUDIT AND GOVERNANCE COMMITTEE HELD ON 27th JULY 2017

PRESENT: Councillors R Ford (Vice-Chair), C Cooke, J Faulkner, M Gant and R Kingstone

Officers John Wheatley (Executive Director Corporate Services), Angela Struthers (Head of Internal Audit Services) and Janice Clift (Democratic and Elections Officer)

Visitors John Gregory and Joan Barnett (Grant Thornton)

21 APOLOGIES FOR ABSENCE

Apologies for absence were received from Councillors M Greatorex and M Summers

22 MINUTES OF THE PREVIOUS MEETING

The minutes of the meeting held on 1 June 2017 were approved and signed as a correct record.

(Moved by Councillor J Faulkner and seconded by Councillor C Cooke)

23 DECLARATIONS OF INTEREST

There were no declarations of Interest.

24 THE AUDIT FINDINGS REPORT

RESOLVED: The Audit Findings for Tamworth Borough Council were presented to the Members by Grant Thornton and a discussion followed

(Moved by Councillor R Ford and seconded by Councillor J Faulkner)

25 MANAGEMENT REPRESENTATION LETTER 2016/17

A Management Representation Letter was submitted to the Members by the Executive Director Corporate Services

RESOLVED: That the letter of representation was approved and agreed by Members

(Moved by Councillor J Faulkner and seconded by Councillor R Ford)

26 ANNUAL STATEMENT OF ACCOUNTS AND REPORT 2016/17

The Corporate Director Executive Services requested Members to approve the Statement of Accounts (the Statement) for the financial year ended 31st March 2017 following completion of the external audit.

RESOLVED: That the Members approved the Annual Statement of Accounts 2016/17 and thanks was given to all of those involved with the Accounts

(Moved by Councillor J Faulkner and seconded by Councillor M Gant)

27 INTERNAL AUDIT CUSTOMER SATISFACTION SURVEY

The Head of Internal Audit Services reported on the outcome of Internal Audit's customer satisfaction survey.

RESOLVED: That the Members Committee considered the report and had no issues to raise.

(Moved by Councillor R Ford and seconded by Councillor C Cooke)

28 INTERNAL AUDIT UPDATE REPORT 2017/18

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 1st Quarter of 2017/18 – and provided members with assurance of the on-

going effective operation of an Internal Audit function and enable any particularly significant issues to be brought to the Committee's attention.

RESOLVED: That the Members considered the report and had no issues to raise.

(Moved by Councillor R Ford and seconded by Councillor C Cooke)

29 RISK MANAGEMENT UPDATE 2017/18

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

RESOLVED: That the Members endorsed the Corporate Risk Register.

(Moved by Councillor R Ford and seconded by Councillor C Cooke)

30 QUARTERLY RIPA REPORT

The Report of the Solicitor to the Council and Monitoring Officer updated Members on the Council's Code of Practice for carrying out surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) specifying that quarterly reports will be taken to Audit and Governance Committee to demonstrate to elected members that the Council is complying with its own Code of Practice when using RIPA.

RESOLVED: That the Members endorsed the RIPA monitoring report for the quarter to 30 June 2017.

(Moved by Councillor R Ford and seconded by Councillor J Faulkner)

31 AUDIT AND GOVERNANCE COMMITTEE TIMETABLE

The Committee reviewed the timetable.

Chair

The Annual Audit Letter for Tamworth Borough Council

Year ended 31 March 2017

September 2017

John Gregory

Director and Engagement Lead

T 0121 232 5333

E john.gregory@uk.gt.com

Joan Barnett

Engagement Manager

T 0121 232 5399

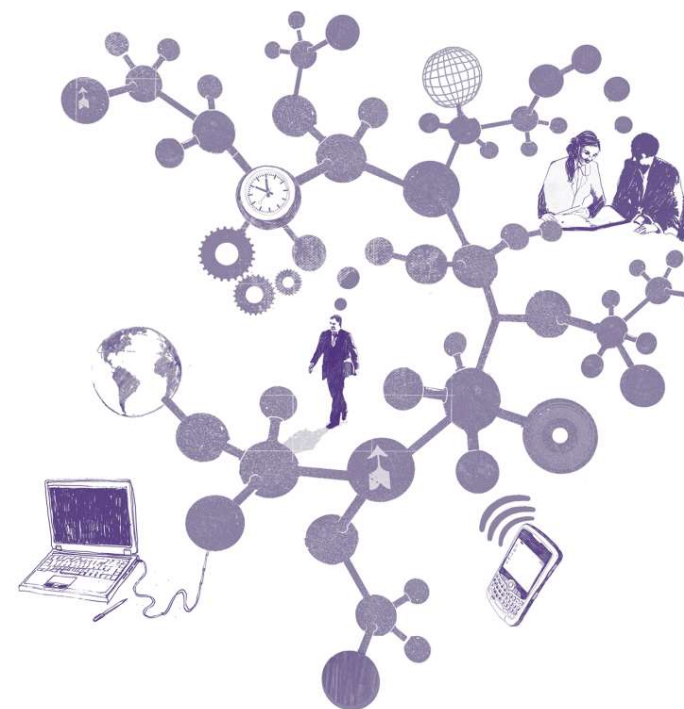
E joan.m.barnett@uk.gt.com

Denise Mills

In charge auditor

T 0121 232 5306

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



Contents

Section	Page
1. Executive summary	3
2. Audit of the accounts	5
3. Value for Money conclusion	10

Appendices

A Reports issued and fees

Page 6

Executive summary

Purpose of this letter

Our Annual Audit Letter (Letter) summarises the key findings arising from the work we have carried out at Tamworth Borough Council (the Council) for the year ended 31 March 2017.

This Letter provides a commentary on the results of our work to the Council and its external stakeholders, and highlights issues we wish to draw to the attention of the public. In preparing this letter, we have followed the National Audit Office (NAO)'s Code of Audit Practice (the Code) and Auditor Guidance Note (AGN) 07 – 'Auditor Reporting'.

We reported the detailed findings from our audit work to the Council's Audit and Governance Committee (as those charged with governance) in our Audit Findings Report on 27 July 2017.

Our responsibilities

We have carried out our audit in accordance with the NAO's Code of Audit Practice, which reflects the requirements of the Local Audit and Accountability Act 2014 (the Act). Our key responsibilities are to:

- give an opinion on the Council's financial statements (section two)
- assess the Council's arrangements for securing economy, efficiency and effectiveness in its use of resources (the value for money conclusion) (section three).

In our audit of the Council's financial statements, we comply with International Standards on Auditing (UK and Ireland) (ISAs) and other guidance issued by the NAO.

Our work

Financial statements opinion

We gave an unqualified opinion on the Council's financial statements on 27 July 2017.

Value for money conclusion

We were satisfied that the Council put in place proper arrangements to ensure economy, efficiency and effectiveness in its use of resources during the year ended 31 March 2017. We reflected this in our audit opinion on 27 July 2017.

Certificate

We certified that we had completed the audit of the accounts of Tamworth Borough Council in accordance with the requirements of the Code on 27 July 2017.

Certification of grants

We also carry out work to certify the Council's Housing Benefit subsidy claim on behalf of the Department for Work and Pensions. Our work on this claim is not yet complete and will be finalised by 30 November 2017. We will report the results of this work to the Audit and Governance Committee in our Annual Certification Letter.

Working with the Council

We are really pleased to have worked with you over the past year. Some examples of where we have worked with you include:

An efficient audit – we delivered the accounts audit to the timescales agreed in advance. The earlier audit deadline of 31 July was achieved a year ahead of when this is mandated in 2018.

Understanding your operational health – through the value for money conclusion we provided you with assurance on your operational effectiveness.

Sharing our insight – we provided independent external audit commentary and insight in your key issues through senior attendance at every Audit Committee. We have also shared with you our insights on various accounting issues including earlier closure timetables.

We would like to record our appreciation for the assistance and co-operation provided to us during our audit by the Council's staff.

Grant Thornton UK LLP
September 2017

Audit of the accounts

Our audit approach

Materiality

In our audit of the Council's accounts, we applied the concept of materiality to determine the nature, timing and extent of our work, and to evaluate the results of our work. We define materiality as the size of the misstatement in the financial statements that would lead a reasonably knowledgeable person to change or influence their economic decisions.

We determined materiality for our audit of the Council's accounts to be £1,081,000, which is 2% of the Council's gross revenue expenditure. We used this benchmark, as in our view, users of the Council's accounts are most interested in how it has spent the income it has raised from taxation and grants during the year.

We also set a lower level of specific materiality of £20,000 for related party transactions; and for disclosures of officers' remuneration, salary bandings and exit packages in the notes to the financial statements.

We set a lower threshold of £54,000, above which we reported errors to the Audit and Governance Committee in our Audit Findings Report.

The scope of our audit

Our audit involves obtaining enough evidence about the amounts and disclosures in the financial statements to give reasonable assurance they are free from material misstatement, whether caused by fraud or error. This includes assessing whether:

- the Council's accounting policies are appropriate, have been consistently applied and adequately disclosed;
- significant accounting estimates made by the Executive Director Corporate Services are reasonable; and
- the overall presentation of the financial statements gives a true and fair view.

We also read the narrative report and annual governance statement to check they are consistent with our understanding of the Council and with the accounts included in the Statement of Accounts on which we gave our opinion.

We carry out our audit in line with ISAs (UK and Ireland) and the NAO Code of Audit Practice. We believe the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Our audit approach was based on a thorough understanding of the Council's business and is risk based.

We identified key risks and set out overleaf the work we performed in response to these risks and the results of this work.

Audit of the accounts – where we focused more of our work

These are the risks which had the greatest impact on our overall strategy and where we focused more of our work.

Risks identified in our audit plan	How we responded to the risk	Findings and conclusions
<p>The revenue cycle includes fraudulent transactions</p> <p>Under ISA (UK&I) 240 there is a presumed risk that revenue may be misstated due to the improper recognition of revenue.</p> <p>This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.</p>	<p>Having considered the risk factors set out in ISA240 and the nature of the revenue streams at Tamworth Borough Council, we determined that the risk of fraud arising from revenue recognition can be rebutted, because:</p> <ul style="list-style-type: none"> • there is little incentive to manipulate revenue recognition • opportunities to manipulate revenue recognition are very limited • the culture and ethical frameworks of local authorities, including Tamworth Borough Council, mean that all forms of fraud are seen as unacceptable 	<p>Our audit work did not identify any issues in respect of revenue recognition.</p>
<p>Valuation of pension fund net asset</p> <p>The Council's pension fund net asset and liability as reflected in its balance sheet represent a significant estimate in the financial statements.</p>	<p>We:</p> <ul style="list-style-type: none"> • identified the controls put in place by management to ensure that the pension fund liability is not materially misstated. We will also assessed whether these controls were implemented as expected and whether they are sufficient to mitigate the risk of material misstatement. • reviewed the competence, expertise and objectivity of the actuary who carried out your pension fund valuation. We gained an understanding of the basis on which the valuation is carried out. • undertook procedures to confirm the reasonableness of the actuarial assumptions made. • reviewed the consistency of the pension fund asset and liability and disclosures in notes to the financial statements with the actuarial report from your actuary. 	<p>Our audit work did not identify any issues in respect of the valuation of the pension fund liability.</p>

Audit of the accounts – where we focused more of our work (continued)

Risks identified in our audit plan	How we responded to the risk	Findings and conclusions
<p>Changes to the presentation of local authority financial statements</p> <p>CIPFA's 'Telling the Story' project, for which the aim was to streamline the financial statements and improve accessibility to the user resulted in changes to the 2016/17 Code of Practice.</p> <p>The changes affected the presentation of income and expenditure in the financial statements and associated disclosure notes. A prior period adjustment (PPA) to restate the 2015/16 comparative figures was also required.</p>	<p>We:</p> <ul style="list-style-type: none"> documented and evaluated the process for the recording the required financial reporting changes to the 2016/17 financial statements. reviewed the re-classification of the Comprehensive Income and Expenditure Statement (CIES) comparatives to ensure that they were in line with the Authority's internal reporting structure. reviewed the appropriateness of the revised grouping of entries within the Movement In Reserves Statement (MIRS). tested the classification of income and expenditure for 2016/17 recorded within the Cost of Services section of the CIES. tested the completeness of income and expenditure by reviewing the reconciliation of the CIES to the general ledger. tested the classification of income and expenditure reported within the new Expenditure and Funding Analysis (EFA) note to the financial statements. reviewed the new segmental reporting disclosures within the 2016/17 financial statements to ensure compliance with the CIPFA Code of Practice 	<p>We were satisfied that the CIES and MIRS were appropriately restated; the accounting entries in 2016/17 were materially fairly stated; and that segmental reporting complied with the CIPFA Code of Practice.</p> <p>We agreed with management that a PPA note to restate the 2015/16 comparative figures was required to fully comply with the Code.</p>
<p>Employee remuneration</p> <p>Payroll expenditure represents a significant percentage of the Council's gross expenditure.</p> <p>We identified the completeness of payroll expenditure in the financial statements as a risk requiring particular audit attention:</p> <ul style="list-style-type: none"> Employee remuneration accruals understated (Remuneration expenses not correct) 	<p>We:</p> <ul style="list-style-type: none"> reviewed and documented the control environment for employee remuneration and performed walkthrough testing to ensure controls in place had been functioning effectively in the period tested the payroll reconciliation to ensure that the payroll system could be agreed to the ledger and financial statements. reviewed the monthly trend analysis of total payroll. tested a sample of employee remuneration payments covering the period 1/4/16 to 31/3/17 to ensure they were accurately accounted for. tested other payroll disclosure such as senior officer remuneration and exit packages. 	<p>Our audit work did not identify any issues in relation to the risk identified.</p>

Audit of the accounts – where we focused more of our work (continued)

Risks identified in our audit plan	How we responded to the risk	Findings and conclusions
<p>Operating expenses Non-pay expenditure represents a significant percentage of the Council's gross expenditure. Management uses judgement to estimate accruals of un-invoiced non-pay costs.</p> <p>We identified the completeness of non- pay expenditure in the financial statements as a risk requiring particular audit attention:</p> <ul style="list-style-type: none"> • Creditors understated or not recorded in the correct period (Operating expenses understated) 	<p>We:</p> <ul style="list-style-type: none"> • reviewed and documented the control environment for operating expenses and performed walkthrough testing to ensure controls in place had been functioning effectively in the period • undertook cut off testing of purchase orders and goods received notes • reviewed the year end accruals process • reviewed the year end control account reconciliations • tested payments after year end to gain assurance there were no material unrecorded liabilities • tested a sample of operating expenses covering the year to ensure they were accurately accounted for. • tested of a sample of creditor balances as at 31/3/17. 	<p>Our audit work did not identify any issues in relation to operating expenses, except:</p> <ul style="list-style-type: none"> • we identified that debtors and creditors were each understated by £93k (the net position was not affected) and • our view that creditors were potentially overstated by £258k as no supporting documentation could be provided to support the potential clawback of the unspent element of a coalfield grant received in 2007

Audit of the accounts

Audit opinion

We gave an unqualified opinion on the Council's accounts on 27 July 2017, in advance of the 30 September 2017 national deadline.

The Council made the accounts available for audit in line with the agreed timetable, and provided a good set of supporting working papers. The finance team responded promptly and efficiently to our queries during the audit.

Key findings arising from the audit of the accounts

We did not identify any adjustments affecting the Council's reported financial position. The draft financial statements for the year ended 31 March 2017 recorded net expenditure of £6,177k and there was no change in the audited accounts. We also recommended a number of adjustments to improve the presentation of the financial statements. The most significant of these was the inclusion in the audited accounts of a Prior Period Adjustment (PPA) note which disclosed the changes made to gross expenditure, gross income, and net expenditure figures reported in 2015/16 to these figures as restated in the accounts for the year ended 31 March 2017.

The other key messages arising from our audit of the Council's financial statements were:

- Our testing of creditors identified one item valued £258k for which no supporting document could be supplied. From discussion with officers we understand this relates to the unspent amount of a Coalfields grant received in 2007 that may be subject to clawback. The officer that administered the grant has now left, and as it is 10 years old no supporting documentation can be found. Management prefers to retain this creditor in case it is asked to repay the unspent amount. We understand Management will be reviewing this in 2017/18.
- We identified that debtors and creditors were understated by £93k. The net value was not affected. This is not a material amount

- In relation to valuation of the housing stock, three of the valuations on the Beacon property valuation certificates had not been entered correctly in the fixed asset register and Asset Management System, resulting in overall error of £57,400. Due to the small value, management agreed to correct this in 2017/18. We were satisfied this was not a material issue for the accounts (net book value of council dwellings is £160.484m).

Annual Governance Statement and Narrative Report

We are required to review the Council's Annual Governance Statement and Narrative Report. It published them on its website with the draft accounts in line with the national deadlines.

Both documents were prepared in line with the relevant guidance and were consistent with the supporting evidence provided by the Council and with our knowledge of the Council.

Value for Money conclusion

Background

We carried out our review in accordance with the NAO Code of Audit Practice (the Code), following the guidance issued by the NAO in November 2016 which specified the criterion for auditors to evaluate:

In all significant respects, the audited body takes properly informed decisions and deploys resources to achieve planned and sustainable outcomes for taxpayers and local people.

Findings

Our first step in carrying out our work was to perform a risk assessment and identify the key risks where we concentrated our work.

We carried out our initial risk assessment based on the NAO's auditor's guidance note (AGN03) and reported to you in our Audit Plan presented on 28 March 2017 that we had not identified any significant risks from our initial risk assessment.

We continued our review of relevant documents, including reviewing your Annual Governance Statement up to the date of giving our auditors report, and did not identify any further significant risks where we needed to perform further work.

Overall VfM conclusion

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 2017.

Appendix A: Reports issued and fees

We confirm below our final fees charged for the audit and provision of non-audit services.

Fees

	Proposed fee £	Actual fees £	2015/16 fees £
Statutory audit of the Council	49,838	49,838	49,838
Housing Benefit Grant Certification *	11,643	TBC	11,575
Total fees (excluding VAT)	61,481	TBC	61,413

The proposed fees for the year were in line with the scale fee set by Public Sector Audit Appointments Ltd (PSAA).

* this is the indicative fee set by Public Sector Audit Appointments Ltd (PSAA). The final fee shall be confirmed on completion of the work in November 2017. Any fee variations are subject to approval by PSAA.

Reports issued

Report	Date issued
Audit Plan	30 March 2017
Audit Findings Report	27 July 2017
Annual Audit Letter	September 2017

Fees for other services

Service	Fees £
Audit related services – Pooling of Housing Capital Receipts certification work indicative fee (final fee to be confirmed on completion of the work in November 2017)	2,500

Non- audit services

- For the purposes of our audit we have made enquiries of all Grant Thornton UK LLP teams providing services to the Council. The table above summarises all other services which were identified.
- We have considered whether other services might be perceived as a threat to our independence as the Council's auditor and have ensured that appropriate safeguards are put in place, as set in the table overleaf.

Reports issued and fees continued

We have considered whether other services might be perceived as a threat to our independence as the Council's auditor and have ensured that appropriate safeguards have been applied to mitigate these risks.

	Service provided to	Fees	Threat identified	Safeguards
Audit related services				
Pooling of Housing Capital Receipts certification work	Tamworth Borough Council	2,500 (indicative)	Self-interest	This is a recurring fee and therefore high self-interest threat. However, the level of this recurring fee taken on its own is not considered a significant threat to independence as the indicative fee for this work of £2,500.00 in comparison to the total fee for the audit of £49,838.00 and in particular to GTUK's turnover overall. Further, the work is on audit related services. It is a fixed fee and there is no contingent element to it. These factors all mitigate the perceived self-interest threat to an acceptable level.
	TOTAL	£2,500		

The above non-audit services are consistent with the Council's policy on the allotment of non-audit work to your auditor and have been approved by the Audit and Governance Committee.



© 2017 Grant Thornton UK LLP. All rights served.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International LTD (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL, and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grant-thornton.co.uk

This page is intentionally left blank

Audit and Governance Committee Update Tamworth Borough Council Progress Report and Update

26 October 2017

Page 19

John Gregory

Engagement Lead

T 0121 232 5333

E john.gregory@uk.gt.com

Joan Barnett

Audit Manager

T 0121 232 5399

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

Denise Mills

In Charge Auditor

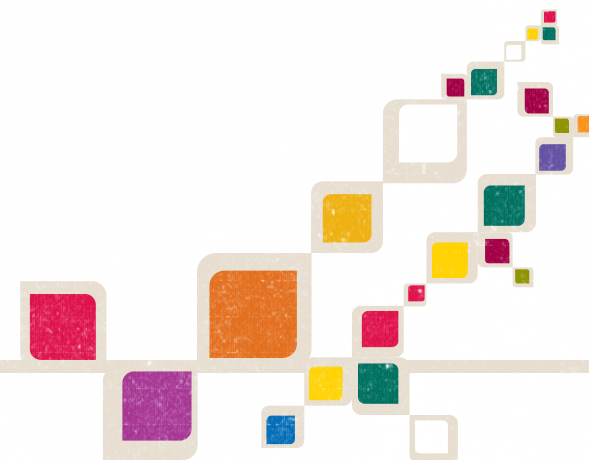
T 0121 232 5306

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



Agenda Item 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.



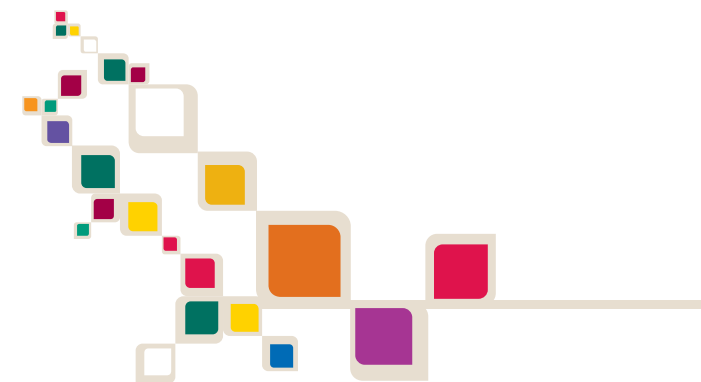
Introduction

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

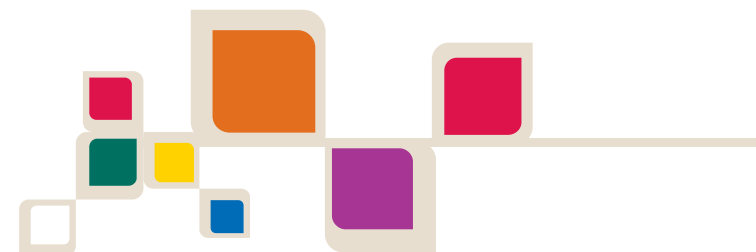
Members of the Audit and Governance Committee can find further useful material on our website www.grant-thornton.co.uk, where we have a section dedicated to our work in the public sector. Here you can download copies of our publications and articles, including the reports mentioned in this update along with other items:

- Income generation is an increasingly essential part of providing sustainable local services ; <http://www.grantthornton.co.uk/en/insights/the-income-generation-report-local-leaders-are-ready-to-be-more-commercial/>
- Social enterprises are becoming increasingly common vehicles for delivering services that are not an ‘essential’ service for an authority but still important to the local community; <http://www.grantthornton.co.uk/en/insights/a-guide-to-setting-up-a-social-enterprise/>
- Fraud risk, 'adequate procedures', and local authorities; <http://www.grantthornton.co.uk/en/insights/fraud-risk-adequate-procedures-and-local-authorities/>
- Brexit and local government; <http://www.grantthornton.co.uk/en/insights/a-global-britain-needs-more-local-government-not-less/> and <http://www.grantthornton.co.uk/en/insights/brexit-local-government--transitioning-successfully/>

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 Engagement Manager.



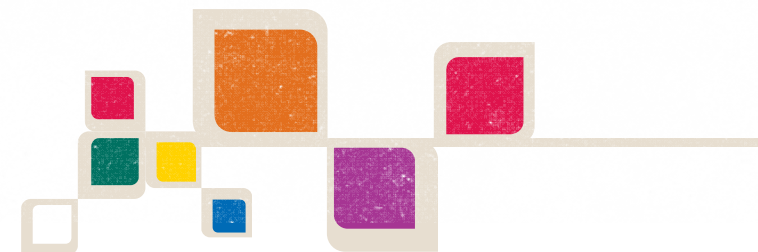
Progress at 26 October 2017



Page 22

2016/17	Planned Date	Complete?	Comments
<p>Annual Audit Letter</p> <p>The annual audit letter (AAL) is being presented to the committee today. The work on the Housing Benefits claim is ongoing. The work will be completed by the deadline of 30 November and we will report our findings in the certification report in January 2018</p>	<p>26 October 2017 for AAL</p> <p>30 November 2017 (HB)</p>	<p>Yes</p> <p>Not yet due</p>	<p>The AAL completed our audit duties for the year.</p> <p>Our housing benefits work is on track for completion by the deadline.</p>
2017/18	Planned Date	Complete?	Comments
<p>Fee Letter</p> <p>We were required to issue a 'Planned fee letter for 2017/18 by the end of April 2017. This is the final audit year under the current contract. PSAA has awarded contracts to audit suppliers and is currently consulting on local appointments. Your audit supplier from 2018/19 will be confirmed by the end of December 2017.</p>	<p>April 2017</p>	<p>yes</p>	<p>We sent our fee letter to Tony Goodwin on 29 March 2017.</p>
<p>Accounts Audit Plan</p> <p>We will issue a detailed accounts audit plan to the Council setting out our proposed approach the audit of the Council's 2017/18 financial statements. This will be issued upon completion of our audit planning.</p> <p>The statutory deadline for the issue of the 2017/18 opinion is brought forward by two months to 31 July 2018. We will discuss with your officers our plan and timetable to ensure that we complete our work by this earlier deadline. You are in a good position to achieve this deadline, having achieved early sign off in 2016/17.</p> <p>We may also need to discuss and agree with you arrangements for the issue of the draft Audit Findings Report, in view of the time available to complete our work and your committee report deadlines.</p>	<p>March 2018</p>	<p>Not yet due</p>	<p>We will present our Audit Plan to the March 2018 meeting of the Committee.</p>

Progress at 26 October 2017



Page 23

2017/18	Planned Date	Complete?	Comments
<p>Interim accounts audit</p> <p>Our interim fieldwork visit plan will reflect the need to complete as much as possible earlier in the audit cycle. Our work will include:</p> <ul style="list-style-type: none"> • 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 • Value for Money conclusion risk assessment. 	<p>January to March 2018 exact dates to be confirmed</p>	<p>Not yet due</p>	<p>We will report the results of our interim work to the Committee either in March 2018 or in June 2018 depending on the timing of this work and the Committee meeting.</p>
<p>Final accounts audit</p> <ul style="list-style-type: none"> • proposed opinion on the Council's accounts • proposed Value for Money conclusion • review of the Council's disclosures in the consolidated accounts against the Code of Practice on Local Authority Accounting in the United Kingdom 2017/18 	<p>June/July 2018 exact dates to be confirmed</p>	<p>Not yet due</p>	<p>We will agree the exact timing of this visit with your Officers</p>
<p>Value for Money (VfM) conclusion</p> <p>The scope of our work is unchanged to last year and is set out in the final guidance issued by the National Audit Office in November 2015. The Code requires auditors to satisfy themselves that; "the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources".</p> <p>The guidance confirmed the overall criterion as; "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".</p> <p>The three sub criteria for assessment to be able to give a conclusion overall are:</p> <ul style="list-style-type: none"> • Informed decision making • Sustainable resource deployment • Working with partners and other third parties 	<p>July 2018</p>	<p>Not yet due</p>	<p>We aim to complete as much of this work as possible by the end of March 2018. We will keep the Council's arrangements and any relevant developments under review until we issue our value for money conclusion at the end of July 2018.</p>

Technical Matters

Page 24



Code of Practice on Local Authority Accounting in the United Kingdom 2017/18 and forthcoming provisions for IFRS 9 and IFRS 15

Code of Practice on Local Authority Accounting in the United Kingdom 2017/18

CIPFA/LASAAC has issued the Local Authority Accounting Code for 2017/18. The main changes to the Code include:

- amendments to section 2.2 (Business Improvement District Schemes (England, Wales and Scotland), Business Rate Supplements (England), and Community Infrastructure Levy (England and Wales)) for the Community Infrastructure Levy to clarify the treatment of revenue costs and any charges received before the commencement date
- amendment to section 3.1 (Narrative Reporting) to introduce key reporting principles for the Narrative Report
- updates to section 3.4 (Presentation of Financial Statements) to clarify the reporting requirements for accounting policies and going concern reporting
- changes to section 3.5 (Housing Revenue Account) to reflect the Housing Revenue Account (Accounting Practices) Directions 2016 disclosure requirements for English authorities
- following the amendments in the Update to the 2016/17 Code, changes to sections 4.2 (Lease and Lease Type Arrangements), 4.3 (Service Concession Arrangements: Local Authority as Grantor), 7.4 (Financial Instruments – Disclosure and Presentation Requirements)

- amendments to section 6.5 (Accounting and Reporting by Pension Funds) to require a new disclosure of investment management transaction costs and clarification on the approach to investment concentration disclosure.

Forthcoming provisions for IFRS 9 and IFRS 15

CIPFA/LASAAC has issued 'Forthcoming provisions for IFRS 9 Financial Instruments and IFRS 15 Revenue from Contracts with Customers in the Code of Practice on Local Authority Accounting in the United Kingdom 2018'. It sets out the changes to the 2018/19 Code in respect of IFRS 9 Financial Instruments and IFRS 15 Revenue from Contracts with Customers. It has been issued in advance of the 2018/19 Code to provide local authorities with time to prepare for the changes required under these new standards.

IFRS 9 replaces IAS 39 Financial Instruments: Recognition and Measurement. IFRS 9 includes a single classification approach for financial assets, a forward looking 'expected loss' model for impairment (rather than the 'incurred loss' model under IAS 39) and some fundamental changes to requirements around hedge accounting.

Technical Matters

Questions:

- Is your Director of Finance aware of the changes to the Code of Practice in 2017/18 and the forthcoming changes to lease accounting and revenue recognition?

IFRS 15 replaces IAS 18 Revenue and IAS 11 Construction Contracts. IFRS 15 changes the basis for deciding whether revenue is recognised at a point in time or over a period of time and introduces five steps for revenue recognition.

It should be noted that the publication does not have the authority of the Code and early adoption of the two standards is not permitted by the 2017/18 Code.

Sector issues

Page 26



Independent Review of Building Regulations and Fire Safety

Sector Issues

The Government has published the terms of reference for the independent Review of Building Regulations and Fire Safety, commissioned following the Grenfell Tower fire tragedy.

The DCLG press release states:

“This Review will urgently assess the effectiveness of current building and fire safety regulations and related compliance and enforcement issues, with a focus on multi occupancy high rise residential buildings. This will include addressing whether the government’s large-scale cladding system testing programme identified any potential systemic failures.

The Review’s 2 key priorities are to develop a more robust regulatory system for the future and provide further assurance to residents that the buildings they live in are safe and remain safe. While the Review will cover the regulatory system for all buildings, it will have a specific focus on multi occupancy high rise residential buildings.

Dame Judith Hackitt, a qualified engineer with strong regulatory background, is leading the Review and will draw on the experience of local government, industry, the fire sector, international experts and MPs. She will also engage with residents of multi occupancy residential buildings.

The Review will report jointly to Communities Secretary Sajid Javid and Home Secretary Amber Rudd. An interim report will be submitted in autumn 2017 and a final report submitted in spring 2018. The Review will co-operate fully with the Public Inquiry, and Dame Judith Hackitt will review her recommendations in the light of the findings of the Inquiry.”

The terms of reference state that the review will:

- map the current regulatory system (i.e. the regulations, guidance and processes) as it applies to new and existing buildings through planning, design, construction, maintenance, refurbishment and change management;
- consider the competencies, duties and balance of responsibilities of key individuals within the system in ensuring that fire safety standards are adhered to;
- assess the theoretical coherence of the current regulatory system and how it operates in practice
- compare this with other international regulatory systems for buildings and regulatory systems in other sectors with similar safety risks;
- make recommendations that ensure the regulatory system is fit for purpose with a particular focus on multi-occupancy high-rise residential buildings.

The full terms of reference are available at:

<https://www.gov.uk/government/publications/independent-review-of-building-regulations-and-fire-safety-terms-of-reference>

Procurement of external audit services



Procurement outcome

As a result of the highly successful procurement of auditor services, opted-in Local government and police bodies throughout England will collectively benefit from reduced fees for audit services in 2018/19 compared to 2016/17. Aggregate savings are expected to exceed £6 million per annum, equivalent to a reduction of approximately 18% in the scale fees payable by local bodies.

The results of the process announced on 20 June 2017 involve the award of the following contracts:

- Lot 1 of approx. £14.6 million per audit year was awarded to Grant Thornton LLP;
- Lot 2 of approx. £10.9 million per audit year was awarded to EY LLP;
- Lot 3 of approx. £6.6 million per audit year to awarded to Mazars LLP;
- Lot 4 of approx. £2.2 million per audit year to awarded to BDO LLP;
- Lot 5 of approx. £2.2 million per audit year to awarded to Deloitte LLP; and
- Lot 6 with no guaranteed value of work to awarded to a consortium of Moore Stephens LLP and Scott-Moncrieff LLP.

Contracts were awarded on the basis of most economically advantageous tender with 50% of the available score awarded to price and 50% awarded to quality.

The procurement strategy, agreed by the PSAA Board in December 2016, sets out the basis on which the procurement of audit services was carried out.

Having concluded the procurement, PSAA will commence the process of appointing auditors to opted-in bodies. For more information on the auditor appointment process [click here](#).

Sector Issues

Finalising and confirming appointments

The PSAA Board will approve all proposed appointments from 2018/19, following consultation with audited bodies, at its meeting in mid-December. The Board's decision on the appointment of auditors is final. Following Board consideration, we will write to each audited body to confirm their appointment. We plan to send all confirmations on 18 December..



Housing Benefit (Subsidy) Assurance Process 2018/19: Module 1 Special Purpose Framework Instruction:

This Circular sets out the arrangements for the audit of the housing benefits subsidy for 2018/19. It is for the LA to appoint a reporting accountant to undertake this work and notify the DWP of this. A standard letter of notification for the LA use is set out in Appendix 1. This letter of notification must be issued to the DWP by the LA no later than the 1st March 2018.

Local Authority 2016/17 Revenue Expenditure and Financing

Sector Issues

DCLG has produced a summary of Local Authorities' 2016/17 provisional revenue spending and financing. It notes that Local government expenditure accounts for almost a quarter of all government spending and the majority of this is through local authority revenue expenditure. The summary is compiled from the Revenue Outturn (RO) returns submitted by all local authorities in England. Coverage is not limited to local councils in England and includes other authority types such as Police and Crime Commissioners and Fire authorities.

The headline messages include:

- Page 29
- Local authority revenue expenditure totalled £93.5 billion for all local authorities in England in 2016-17. This was 1.1% lower than £94.5 billion spent over 2015-16.
 - Expenditure on Adult Social Care increased to £14.9 billion in 2016-17. This was £0.5 billion (3.6%) higher than in 2015-16. 2016-17 was first year local authorities were able to raise additional funding for Adult Social Care through the council tax precept.
 - The largest decrease in local authority expenditure was on Education services. This was £0.8 billion (2.4%) lower in 2016-17 than in 2015-16. The majority of this decrease is due to local authority funded schools converting to academies.
 - Local authorities are financing more of their expenditure from locally retained income. 40.4% of revenue expenditure was funded through council tax and retained business rates and 57.5% from central Government grants. The remaining 2.1% was funded by reserves and collection fund surpluses. These percentages were 38.7%, 60.4% and 0.9% respectively in 2015-16.
 - Local authorities used £1.5 billion (6.2%) of the £24.6 billion reserves balance held at the start of the 2016-17.
 - Local authorities' use of reserves was £1.1 billion higher in 2016-17 than in 2015-16. Due to changes in their capital programme, £0.5 billion of this increase is due to the Greater London Authority.

The full report is available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639755/Revenue_Expenditure_and_Financing_2016-17_Provisional_Outturn.pdf

Did you know....

This data set and many others are included in CFO Insights.

CFO Insights is the Grant Thornton and CIPFA online analysis tool. It gives those aspiring to improve the financial position of their organisation instant access to insight on the financial performance, socio-economic context and service outcomes of theirs and every other council in England, Scotland and Wales.

More information is available at:

<http://www.cfoinsights.co.uk/>

Grant Thornton publications

Page 30



Combined Authorities: Signs of Success

In her foreword to 'Building our Industrial Strategy' the Prime Minister states that the initiative "will help to deliver a stronger economy and a fairer society – where wealth and opportunity are spread across every community in our United Kingdom, not just the most prosperous places in London and the South East."

Combined Authorities (CAs) – the newest model for the governance of local public services – are central to this.

In response to this, Grant Thornton and Bond Dickinson have jointly commissioned a report which provides an insight into the establishment of each combined authority in the context of their specific challenges. It is still early days for most combined authorities – the political and administrative difficulties of adopting this model are not to be under-estimated - but early signs are emerging of their potential to innovate and drive success.

The report benchmarks combined authorities using key indicators of growth, housing, transport and skills amongst others. We have also used our Vibrant Economy Index, which goes beyond financial returns and takes into account the wellbeing of society, to compare city regions. We believe that these benchmarks can serve as a baseline for assessment of progress over time.

Key findings from the report:

- CAs must begin to reduce the institutional blurring with historic local government structures that has occurred with their formation. As greater clarity emerges over their roles, functions, and profiles of individual mayors, ; their perceived legitimacy will increase.
- CAs stand and fall on their ability to add value through targeted investment, strategic co-ordination, joined-up policy and the leveraging in of additional resources (particularly additional private sector funds).
- There is no single checklist or set of criteria for measuring the success of mayors and combined authorities, each city region must articulate its own challenges and show progress in tackling them.
- A balanced set of benchmarks encompassing both economic and social success will, however, serve as a useful stimulus for the debate around the impact of the combined authority model over time.

Grant Thornton publications

Questions:

- Have you read our report?



Combined Authorities: signs of success



<http://www.grantthornton.co.uk/en/insights/combined-authorities-signs-of-success/>

Setting up a successful social enterprise

Local government continues to innovate as it reacts to ongoing austerity. An important strand of this response has been the development of alternative delivery models, including local authority trading companies, joint ventures and social enterprises.

This report focuses on social enterprises in local government; those organisations that trade with a social purpose or carry out activities for community benefit rather than private advantage. Social enterprises come in a variety of shapes and sizes as they do not have a single legal structure or ownership rule and can adopt any corporate form as long as it has a social purpose.

In this report we explore what social enterprises look like, the requirements for setting one up, how they should be managed to achieve success and how they can be ended.

We have complemented this with a range of case studies providing inspiring ideas from those that have been successful and some lessons learned to take into consideration.

Key findings from the report:

- Austerity continues to be a key driver for change: social enterprises are a clear choice where there is an opportunity to enhance the culture of community involvement by transferring these services into a standalone entity at its centre
- The social enterprise model tends to lend itself more to community services such as libraries, heritage management and leisure, but not exclusively so
- Social enterprises can open up new routes of funding including the ability to be flexible on pricing and access to pro bono or subsidised advice
- Some local authorities have converted existing models into social enterprises; for example where a greater focus on social outcomes has been identified

Striking a balance between financial and social returns

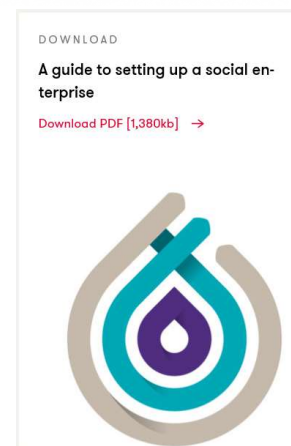
If you are a local authority looking to transition a public service to a social enterprise model certain factors will be key to your success including: leadership, continuing the culture, branding, staff reward and secure income stream.

Download our guide to explore how to handle these factors to ensure success, the requirements for setting up a social enterprise; and how social enterprise can be ended. The guide also showcases a number of compelling case studies from local authorities around England, featuring inspiring ideas from those social enterprises that have been a success; and lessons learned from those that have encountered challenges.

Grant Thornton publications

Questions:

- Is your Council exploring options for delivery of services?
- Have you read our report?
- Have you downloaded our guide?



<http://www.grantthornton.co.uk/en/insights/a-guide-to-setting-up-a-social-enterprise/>

A Manifesto for a Vibrant Economy

Developing infrastructure to enable local growth

Cities and shire areas need the powers and frameworks to collaborate on strategic issues and be able to raise finance to invest in infrastructure priorities. Devolution needs to continue in England across all places, with governance models not being a “one-size-fits all”. Priorities include broadband, airport capacity in the North and east-west transport links.

Addressing the housing shortage, particularly in London and the Southeast, is a vital part of this. There simply is not enough available land on which to build, and green belt legislation, though designed to allow people living in cities space to breath, has become restrictive and is in need of modernisation. Without further provision to free up more land to build on, the young people that we need to protect the future of our economy will not be able to afford housing, and council spending on housing the homeless will continue to rise.

Business rates are also ripe for review – a property-based tax is no longer an accurate basis for taxing the activity and value of local business, in particular as this source of funding becomes increasingly important to the provision of local authority services with the phasing out of the Government’s block grant.

Demographic and funding pressures mean that the NHS no longer remains sustainable, and the integration of health and social care – recognised as critical by all key decision makers – remains more aspiration than reality.

There is an opportunity for communities to take a more holistic approach to health, for example creating healthier spaces and workplaces and tackling air quality, and to use technology to provide more accessible, cheaper diagnosis and treatment for many routine issues

Finding a better way to measure the vibrancy of places

When applied to a place we can see that traditional indicators of prosperity such as GVA, do not tell the full story. To address this we have developed a [Vibrant Economy Index](#) to measure the current and future vibrancy of places. The Index uses the geography of local authority areas and identifies six broad objectives for society: prosperity, dynamism and opportunity, inclusion and equality, health wellbeing and happiness, resilience and sustainability, and community trust and belonging.

The city of Manchester, for example, is associated with dynamic economic success. While our Index confirms this, it also identifies that the Greater Manchester area overall has exceptionally poor health outcomes, generations of low education attainment and deep-rooted joblessness. These factors threaten future prosperity, as success depends on people’s productive participation in the wider local economy, rather than in concentrated pockets.

Every place has its own challenges and opportunities. Understanding what these are, and the dynamic between them, will help unlock everybody’s ability to thrive. Over the coming months we will continue to develop the Vibrant Economy Index through discussions with businesses, citizens and government at a national and local level.

Guy Clifton – Head of Local Government Advisory

Grant Thornton publications

Question:

- Have you read our manifesto?



<http://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/documents/creating-manifesto-vibrant-economy-draft-recommendations.pdf>

The Board: creating and protecting value

Grant Thornton publications

Question:

- Have you read our report?

Value creation	
Non-executives	<p>Directorship How well do the non-executives:</p> <ul style="list-style-type: none"> • design, debate and decide the organisation's future? • inspire and guide the executive to realise the organisation's purpose? • provide support to the executives?
	<p>Leadership How well do the executives:</p> <ul style="list-style-type: none"> • Make decisions aligned with realising the organisation's purpose? • Inspire and motivate employees to realise the organisation's purpose? • model the values of the organisation?
	Executives
Value protection	
	<p>Assurance How well do the non-executives:</p> <ul style="list-style-type: none"> • monitor financial, compliance and business indicators? • ensure appropriate processes are in place to manage risk? • have oversight of the executive team?
	<p>Management How well do the executives:</p> <ul style="list-style-type: none"> • set goals, creating plans and allocating resources to achieve them? • effectively assign roles and responsibilities? • Focus on day-to-day tasks and resources needed to deliver strategic aims?

Source: The Board: Creating and protecting value, 2017, Grant Thornton



<http://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/publication/board-effectiveness-report-2017.pdf>

Page 34

In all sectors, boards are increasingly coming under pressure from both the market and regulators to improve their effectiveness and accountability. This makes business sense given a strong governance culture in the boardroom produces better results, promotes good behaviour within the organisation and drives an organisation's purpose.

Grant Thornton's new report 'The Board: creating and protecting value' is a cross- sector review of board effectiveness, based on a survey of executives and non-executives from a range of organisations including charities, housing associations, universities, local government, private companies and publically listed companies.

It considers the challenges faced by boards, ways in which they can operate more effectively; and how to strike the right balance between value protection and value creation.

This report uses the DLMA analysis which categorises skills into four areas: Directorship, Leadership, Management and Assurance. This powerful tool provides a framework (see graph 1) with which to evaluate how well an organisation is performing in balance of skills and understanding of roles; and responsibilities between the executive and Board. It helps align risk (value protection) and opportunity (value creation) with overarching strategy and purpose.

International Consortium on Governmental Financial Management

Introduction

Grant Thornton and the International Consortium on Governmental Financial Management (ICGFM) partner every other year to perform an international survey of Public Financial Leaders.

In 2015 the theme was innovation in public financial management. This year's survey has been designed to identify and describe emerging issues around transparency and citizen engagement – building on the themes highlighted in the 2015 report.

The insights will be published in a report later in 2017 and we would be delighted if you were able to spend some time completing the brief on-line questionnaire which can be found [here](#). Your Audit Manager will be able to provide you with a link to the survey if required.

Please note that the ICGFM and Grant Thornton will not identify, or attribute thoughts and quotations to, individual survey respondents in the final 2017 report. This preserves your anonymity, so please respond freely, honestly and openly.

We have again partnered with the ICGFM to survey Financial Leaders

Question:

- Have you completed the ICGFM survey on transparency and citizen engagement?



Innovation in public financial management
in an increasingly complex and uncertain global environment

Global financial management leaders survey 2015





© 2017 Grant Thornton UK LLP. All rights reserved

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL).GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grantthornton.co.uk

© 2017 Grant Thornton UK LLP. All rights reserved.

AUDIT & GOVERNANCE COMMITTEE

26 OCTOBER 2017

REPORT OF THE SOLICITOR TO THE COUNCIL AND MONITORING OFFICER

LOCAL GOVERNMENT OMBUDSMAN ANNUAL REVIEW 2016/17

Purpose

To advise the Committee of the views of the Local Government Ombudsman in relation to complaints against the Borough Council and provide an opportunity for members of the Committee to raise any issues they consider appropriate and consider the effectiveness of investigations relating to Tamworth Borough Council.

Recommendation

That the Committee

- 1. endorse the Annual Review Letter as attached at Appendix 1 and**
- 2. acknowledge the change of name in the office of the Ombudsman.**

Executive Summary

In the year 2016/17 the Ombudsman received 7 enquiries and complaints about our authority, and made 8 reported decisions. In 2015/16 the Ombudsman received 13 enquiries and complaints about our authority, and made 14 decisions. In 2014/15 the Ombudsman recorded 11 enquiries and complaints. Apart from an increase in 2013/14 which, as had been suspected, was unusually inflated due to the changes that took place in the Ombudsman's office for recording contact made with them, the position in relation to complaints remains fairly static. In 2012/13 there were 11 complaints.

Of the 7 enquiries and complaints 6 also appear in the decisions report. Of the 8 reported cases in the decisions report, 2 are no more than an enquiry to the Ombudsman Office for which we as the Council receive no notification. However every call and contact to the Ombudsman Office by a member of the public is given a case number and in turn each case has a decision recorded against it. It would be interesting to know how many reported cases across the country are merely enquiries. Of the other 6 cases in the decisions report only 2 resulted in investigations and of those cases only 1 was upheld. In relation to the upheld case the Ombudsman's suggested remedy was invoked.

It is worth noting that the statistical report indicates that the uphold rate for complaints for Tamworth is 50% despite 7 of the 8 remedies being stated by the Ombudsman in his report as NULL.

Two decisions were “referred back for local resolution”, this means that the complaint has been resolved by the Council; three decisions were “closed after initial enquiries” this occurs when the Ombudsman decides it cannot or should not investigate a complaint e.g. the Planning Inspector made the decision therefore it was outside the Ombudsman’s jurisdiction. In one decision advice was given by the Ombudsman office, we do not have any details of the cases nor advice provided. One decision was “not upheld” in this instance the Ombudsman investigated a noise complaint and decided that the Council had not acted with fault.

In June 2016 the Local Government Office issued a press release suggesting that the trend is towards an increase in complaints and an increase in demand putting the Ombudsman Office and local government under pressure. Despite this trend Tamworth Borough Council has experienced a fall in complaints and enquiries to the Ombudsman.

The Ombudsman no longer monitors the average time to respond however we continue to work to the 28 day target.

We recently received communication from the Ombudsman Office of a change of name to the Local Government and Social Care Ombudsman. This was done to highlight that the Ombudsman Office looks at complaints regarding all areas of adult social care – including privately arranged or funded care.

Background Information

The Committee’s Terms of Reference include an overview of the regulatory framework within which the authority works and includes a role of monitoring the effectiveness of Local Government Ombudsmen (LGO) investigations. As the operation of the LGO forms part of this regulatory framework the Committee is provided with the LGO annual review for consideration.

The LGO distribute annual review letters to all councils regarding their performance in dealing with complaints made about them to the Ombudsman. The aim is to provide councils with information to help them improve complaint handling, and improve services more generally, for the benefit of the public. The letters also include a summary of statistics relating to the complaints received by the LGO and dealt with against each council.

The LGO has the power to investigate:
complaints by members of the public who consider that they have been caused injustice by maladministration or service failure in connection with action taken by the Council and certain other bodies in the exercise of its administrative functions. Complaints by members of the public who consider they have sustained injustice during the course of privately arranged or

funded adult social care, and complaints from pupils (or their parents) of injustice in consequence of an act/omission of a head teacher or governing body of a maintained school.

On the whole most complaints about Borough Council matters relate to housing issues.

Whilst the Ombudsman can investigate complaints about how the Council has done something, it cannot question what a Council has done simply because someone does not agree with it.

A complainant must give the Council an opportunity to deal with a Complaint against it first. It is best to use the Council's own complaints procedure, in the first instance, although in practice that is not always the route taken by a complainant. If a complainant is not satisfied with the action the Council takes he or she can send a written complaint to the Local Government Ombudsman, or ask a Councillor to do so on their behalf.

The objective of the Ombudsmen is to secure, where appropriate, satisfactory redress for complainants and better administration for the authorities. Since 1989, the Ombudsmen have had power to issue advice on good administrative practice in local government based on experience derived from their investigations.

The LGO provide each local authority with an annual review of the authority's performance in dealing with complaints against it which were referred to the relevant Ombudsman, so that the authority can learn from its own performance compared to other authorities.

Implications of this report

There are no direct financial/staffing implications or direct implications in relation to community/performance planning, sustainable development, community safety, equal opportunities or human rights arising from this report.

Report Author

Jane M Hackett - Solicitor to the Council and Monitoring Officer
jane-hackett@tamworth.gov.uk Tel; 01827 709258

List of Background papers

Local Government Act 1974 as amended

Appendices

Appendix 1 - Local Government Ombudsman Annual Review Letter 2016

Appendix 2 – spreadsheet providing information on complaints and enquiries received 2016/17

Appendix 3 – spreadsheet providing information on decisions made in 2016/17

20 July 2017

By email

Tony Goodwin
Chief Executive
Tamworth Borough Council

Dear Tony Goodwin,

Annual Review letter 2017

I write to you with our annual summary of statistics on the complaints made to the Local Government and Social Care Ombudsman (LGO) about your authority for the year ended 31 March 2017. The enclosed tables present the number of complaints and enquiries received about your authority and the decisions we made during the period. I hope this information will prove helpful in assessing your authority's performance in handling complaints.

The reporting year saw the retirement of Dr Jane Martin after completing her seven year tenure as Local Government Ombudsman. I was delighted to be appointed to the role of Ombudsman in January and look forward to working with you and colleagues across the local government sector in my new role.

You may notice the inclusion of the '*Social Care Ombudsman*' in our name and logo. You will be aware that since 2010 we have operated with jurisdiction over all registered adult social care providers, able to investigate complaints about care funded and arranged privately. The change is in response to frequent feedback from care providers who tell us that our current name is a real barrier to recognition within the social care sector. We hope this change will help to give this part of our jurisdiction the profile it deserves.

Complaint statistics

Last year, we provided for the first time statistics on how the complaints we upheld against your authority were remedied. This year's letter, again, includes a breakdown of upheld complaints to show how they were remedied. This includes the number of cases where our recommendations remedied the fault and the number of cases where we decided your authority had offered a satisfactory remedy during the local complaints process. In these latter cases we provide reassurance that your authority had satisfactorily attempted to resolve the complaint before the person came to us.

We have chosen not to include a 'compliance rate' this year; this indicated a council's compliance with our recommendations to remedy a fault. From April 2016, we established a new mechanism for ensuring the recommendations we make to councils are implemented, where they are agreed to. This has meant the recommendations we make are more specific, and will often include a time-frame for completion. We will then follow up with a council and seek evidence that recommendations have been implemented. As a result of this new process, we plan to report a more sophisticated suite of information about compliance and service improvement in the future.

This is likely to be just one of several changes we will make to our annual letters and the way we present our data to you in the future. We surveyed councils earlier in the year to find out, amongst other things, how they use the data in annual letters and what data is the most useful; thank you to those officers who responded. The feedback will inform new work to

provide you, your officers and elected members, and members of the public, with more meaningful data that allows for more effective scrutiny and easier comparison with other councils. We will keep in touch with you as this work progresses.

I want to emphasise that the statistics in this letter comprise the data we hold, and may not necessarily align with the data your authority holds. For example, our numbers include enquiries from people we signpost back to the authority, but who may never contact you.

In line with usual practice, we are publishing our annual data for all authorities on our website. The aim of this is to be transparent and provide information that aids the scrutiny of local services.

The statutory duty to report Ombudsman findings and recommendations

As you will no doubt be aware, there is duty under section 5(2) of the Local Government and Housing Act 1989 for your Monitoring Officer to prepare a formal report to the council where it appears that the authority, or any part of it, has acted or is likely to act in such a manner as to constitute maladministration or service failure, and where the LGO has conducted an investigation in relation to the matter.

This requirement applies to all Ombudsman complaint decisions, not just those that result in a public report. It is therefore a significant statutory duty that is triggered in most authorities every year following findings of fault by my office. I have received several enquiries from authorities to ask how I expect this duty to be discharged. I thought it would therefore be useful for me to take this opportunity to comment on this responsibility.

I am conscious that authorities have adopted different approaches to respond proportionately to the issues raised in different Ombudsman investigations in a way that best reflects their own local circumstances. I am comfortable with, and supportive of, a flexible approach to how this duty is discharged. I do not seek to impose a proscriptive approach, as long as the Parliamentary intent is fulfilled in some meaningful way and the authority's performance in relation to Ombudsman investigations is properly communicated to elected members.

As a general guide I would suggest:

- Where my office has made findings of maladministration/fault in regard to routine mistakes and service failures, and the authority has agreed to remedy the complaint by implementing the recommendations made following an investigation, I feel that the duty is satisfactorily discharged if the Monitoring Officer makes a periodic report to the council summarising the findings on all upheld complaints over a specific period. In a small authority this may be adequately addressed through an annual report on complaints to members, for example.
- Where an investigation has wider implications for council policy or exposes a more significant finding of maladministration, perhaps because of the scale of the fault or injustice, or the number of people affected, I would expect the Monitoring Officer to consider whether the implications of that investigation should be individually reported to members.
- In the unlikely event that an authority is minded not to comply with my recommendations following a finding of maladministration, I would always expect the Monitoring Officer to report this to members under section five of the Act. This is an exceptional and unusual course of action for any authority to take and should be considered at the highest tier of the authority.

The duties set out above in relation to the Local Government and Housing Act 1989 are in addition to, not instead of, the pre-existing duties placed on all authorities in relation to Ombudsman reports under The Local Government Act 1974. Under those provisions, whenever my office issues a formal, public report to your authority you are obliged to lay that report before the council for consideration and respond within three months setting out the action that you have taken, or propose to take, in response to the report.

I know that most local authorities are familiar with these arrangements, but I happy to discuss this further with you or your Monitoring Officer if there is any doubt about how to discharge these duties in future.

Manual for Councils

We greatly value our relationships with council Complaints Officers, our single contact points at each authority. To support them in their roles, we have published a Manual for Councils, setting out in detail what we do and how we investigate the complaints we receive. When we surveyed Complaints Officers, we were pleased to hear that 73% reported they have found the manual useful.

The manual is a practical resource and reference point for all council staff, not just those working directly with us, and I encourage you to share it widely within your organisation. The manual can be found on our website www.lgo.org.uk/link-officers

Complaint handling training

Our training programme is one of the ways we use the outcomes of complaints to promote wider service improvements and learning. We delivered an ambitious programme of 75 courses during the year, training over 800 council staff and more 400 care provider staff. Post-course surveys showed a 92% increase in delegates' confidence in dealing with complaints. To find out more visit www.lgo.org.uk/training

Yours sincerely

A handwritten signature in black ink, appearing to read 'M King', with a stylized flourish underneath.

Michael King
Local Government and Social Care Ombudsman for England
Chair, Commission for Local Administration in England

For further information on how to interpret our statistics, please visit our website:
<http://www.lgo.org.uk/information-centre/reports/annual-review-reports/interpreting-local-authority-statistics>

Complaints and enquiries received

Adult Care Services	Benefits and Tax	Corporate and Other Services	Education and Children's Services	Environment Services	Highways and Transport	Housing	Planning and Development	Other	Total
0	1	0	0	2	1	3	0	0	7

Page 44

Decisions made

				Detailed Investigations			
Incomplete or Invalid	Advice Given	Referred back for Local Resolution	Closed After Initial Enquiries	Not Upheld	Upheld	Uphold Rate	Total
0	1	2	3	1	1	50%	8

Notes

Our uphold rate is calculated in relation to the total number of detailed investigations.
 The number of remedied complaints may not equal the number of upheld complaints. This is because, while we may uphold a complaint because we find fault, we may not always find grounds to say that fault caused injustice that ought to be remedied.

Complaints Remedied

by LGO	Satisfactorily by Authority before LGO Involvement
1	0

	Reference	Authority
1	15017189	Tamworth Borough Council
2	16005186	Tamworth Borough Council
3	16010443	Tamworth Borough Council
4	16010962	Tamworth Borough Council
5	16011262	Tamworth Borough Council
6	16016164	Tamworth Borough Council
7	16018853	Tamworth Borough Council

Category	Received
Housing	15-Apr-16
Housing	12-Jul-16
Benefits & Tax	15-Nov-16
Housing	27-Oct-16
Environmental Services & Public Protection & Regulation	03-Nov-16
Highways & Transport	06-Feb-17
Environmental Services & Public Protection & Regulation	21-Mar-17

	Reference	Authority
1	15012243	Tamworth Borough Council
2	15014327	Tamworth Borough Council
3	15017189	Tamworth Borough Council
4	16005186	Tamworth Borough Council
5	16010443	Tamworth Borough Council
6	16010962	Tamworth Borough Council
7	16011262	Tamworth Borough Council
8	16016164	Tamworth Borough Council

Category	Decision Date
Housing	12-May-16
Planning & Development	05-Apr-16
Housing	06-May-16
Housing	12-Jul-16
Benefits & Tax	06-Dec-16
Housing	27-Oct-16
Environmental Services & Public Protection & Regulation	26-Jan-17
Highways & Transport	22-Feb-17

Decision
Upheld
Closed after initial enquiries
Referred back for local resolution
Referred back for local resolution
Closed after initial enquiries
Advice given
Not Upheld
Closed after initial enquiries

Remedy
Apology,Financial Redress,Procedure Change,Additional services
Null
Null
Null
Null
Null
Null
Null

AUDIT & GOVERNANCE COMMITTEE

26 OCTOBER 2017

REPORT OF THE SOLICITOR TO THE COUNCIL AND MONITORING OFFICER

REGULATION OF INVESTIGATORY POWERS ACT 2000

Purpose

To receive the Office of Surveillance Commissioner (OSC) inspection report in relation to the RIPA policy, procedures, documentation and training.

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

- 1. endorse the recommendations of the OSC**
- 2. refer the findings of the report and changes to the RIPA policy to Council for ratification and**
- 3. endorse the RIPA monitoring report for the quarter to 30 September 2017.**

Executive Summary

In July 2017 the Office of the Surveillance Commissioner (OSC) conducted an inspection into the RIPA policy, procedures, documentation and training utilised at the Council. It is recommended that the outcome of the inspection be reported to Council on 12 December 2017 for ratification. The Commissioner reported that the recommendations arising from the previous inspection have been implemented and accepted by the Council. RIPA awareness had been raised throughout the Council, the risk of "status drift" and those posed by usage of social media and amendment to the Procedure and Guidance document. The policy was updated in line with the recommendations of the Commissioner and has since been updated further

on two occasions as a result of changes to legislation and the Codes of Practice published by the Home Office. Training took place in January 2015 and there has been further training events in the past week for officers who previously had no RIPA training and for members with refresher training being delivered for those officers previously trained. The training focused on the use of internet and social media sites to carry out research on persons and the association arising therefrom with surveillance. Training will continue to be delivered through Netconsent. The feedback from the training has been positive and going forward training for RIPA has been added to the Corporate Training Programme.

The Commissioner has recommended from the current inspection that

- guidance regarding use of internet and social networking sites (SNS) for research of persons and how this might meet the requirement as directed surveillance or covert human intelligence sources (CHIS) should be drawn up and actively disseminated to staff.

The amended RIPA policy incorporating the Commissioners recommendation is attached for consideration by the Committee and thereafter referral to Council for ratification on 12 December 2017. The revised policy will be published, a questionnaire shall be issued through Netconsent for all staff and a communication containing guidance will be sent to all staff regarding use of internet and social media sites. The practice that quarterly reports on the use of RIPA powers be submitted to Audit & Governance Committee will continue.

Options Considered

Obligations arising under RIPA for the authority are statutory therefore there 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 respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is 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 and updated in January 2016 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 1 July 2017 to 30 September 2017.

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 2017/18

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

No applications

Background papers

Regulation of Investigatory Powers Act 2000
Home Office Codes of Practice – Covert Surveillance and Covert Human
Intelligence Sources

Appendices

Appendix 1 - OSC Inspection report dated 25 July 2017
Appendix 2 - Draft RIPA policy as amended

*“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”*



OSC/INSP/075

Office of Surveillance
Commissioners

The Rt. Hon. Lord Igor Judge
Chief Surveillance Commissioner
Office of Surveillance Commissioners
PO Box 29105
London
SW1V 1ZU

25th July 2017

OSC INSPECTION – TAMWORTH BOROUGH COUNCIL

Inspector

Graham Wright

Introduction

1. Tamworth Borough Council is one of the geographically smallest council areas. It is situated in the south-west of Staffordshire and has a population of approximately 77,000.
2. The previous inspection of this Council by the OSC was undertaken by His Honour Norman Jones QC in October 2014.
3. The Chief Executive is Mr Anthony Goodwin, whose address for correspondence is Marmion House, Lichfield Street, Tamworth B79 7BZ. Mr Goodwin was in post at the time of the previous inspection in 2014.
4. The RIPA Senior Responsible Officer (SRO) is Mrs Jane Hackett, Solicitor to the Council who was also in post at the time of the earlier inspection and took part in it.
5. Since the last inspection there have been no RIPA authorisations of directed surveillance or covert human intelligence sources (CHIS).
6. I am preparing this report without visiting the Council. I sent the agreed questionnaire which was completed and returned to me along with other requested material. Having considered this material in detail, I have concluded that I can properly report to you without a physical inspection. This is in accordance with your recent direction that not every second-tier district or borough council needs to be visited every three years as a matter of course.

Progress against recommendations/Action Plan

7. The previous inspection made three recommendations, all of which were accepted by the Council.
8. *Raise RIPA awareness throughout the Council.*

Completed: This recommendation was made as there was some concern that there was a lack of awareness among those departments that were unlikely to use RIPA. The RIPA policy has been circulated to all staff, along with a questionnaire to ensure that the policy is read. Staff are required to read the policy and answer the questionnaire prior to logging onto their system.

9. *Address the risks of "status drift" and those posed by the usage of social media.*

Completed: Training in relation to these issues has been provided to staff likely to encounter them. Additionally, the circulation of the RIPA policy addresses the areas of concern. The current policy does not have a section on social media but one is due to be developed by the SRO in the autumn and a full survey undertaken of staff likely to access social media sites which will thereafter be monitored. A recent communication to departments regarding use of surveillance equipment included a question regarding use of social media. In all departments the response indicated that no use is currently being made. **However, I make a specific recommendation regarding the need for advice and guidance in relation to use of the internet and social networking sites.**

10. *Amend the Procedure and Guidance document.*

Completed: The suggested amendments have been made to the current document.

RIPA Structure and Policy

11. Jane Hackett, Solicitor to the Council, is the appointed 'senior responsible officer' and also the RIPA monitoring officer. She maintains the Central Record of authorisations, which is a spreadsheet and contains all the information required by the Code of Practice. No authorisation has been granted since October 2010.
12. There are three appointed and trained authorising officers: the Chief Executive, Executive Director Corporate Services and Corporate Director Growth Assets and Environment.
13. The main policy document is the *Policy and Procedure Regulation of Investigatory Powers Act 2000*. This is in many ways a useful and compliant document. What is lacking is any guidance in relation to use of the internet and social networking sites by council staff to carry out research on persons. In the questionnaire response it was said that a policy will be produced in the autumn but given that this issue was raised during the inspection in 2014 **I am inclined to make this an unequivocal recommendation.**

Reports to Members

14. There is an annual report to the full Council meeting at which the policy is approved. In addition there are quarterly reports to the Audit and Governance Committee.

Liaison with magistrates' court under The Protection of Freedoms Act 2012

15. There have been no authorisations granted since the inception of the Protection of Freedoms Act 2012 but detailed guidance is laid down in the policy document regarding the procedure to be adopted in the unlikely event of an authorisation being granted. Delegated officers will present the authorisation at the local Magistrates Court and the authorising officer should also be prepared to attend. The advice of the Solicitor to the Council is recommended.

Training

16. Since the previous inspection an external provider has conducted training sessions for all authorising officers, the SRO and enforcement/investigative staff. An overview of RIPA has been provided to elected members also. All staff in the Council have had the aforementioned policy and questionnaire sent to them.
17. It is intended to convene training sessions in the autumn.

Social media investigations

18. It is assessed by the SRO that very little use is being made of these media based upon recent responses from departments to a questionnaire sent out by the SRO. Training sessions have emphasised that repeated viewing and interaction with other persons may need authorisation under RIPA.
19. These measures need supporting by a clear and appropriate section of guidance within the policy document and this needs promulgating to all staff.

CCTV

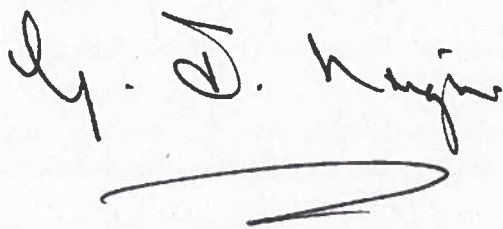
20. The public place CCTV system is wholly owned and managed by Tamworth Borough Council and its staff. There is a protocol with Staffordshire Police in which it is recognised that any use of the system under RIPA should be authorised by the police and details of that authorisation provided to CCTV managers.
21. A full review of the system has been carried out to ensure compliance with the Surveillance Camera Commissioner's Code of Practice and the Third Party Self-Certification Scheme has been completed.

Conclusions

22. Tamworth Borough Council has not granted an authorisation for covert activity under the Regulation of Investigatory Powers Act 2000 since October 2010. The reasons for this position are: a greater reliance on more overt means to investigate cases and carry out enforcement; concern expressed by elected members regarding the frequency of usage of covert activity; the constraints imposed by the Protection of Freedoms Act 2012; and staffing reductions.
23. All these factors have resulted in the Council being very unlikely to use the powers vested under RIPA – albeit that the internet and SNS has the potential to challenge this stance. It is for this reason, and the ease with which staff may unwittingly engage in covert surveillance in the 'virtual world', that I make this a recommendation. It is also incumbent on a council to provide adequate guidance to its staff.
24. With this one exception the regime of guidance, oversight and training at Tamworth is appropriate for their situation and Jane Hackett is an experienced, knowledgeable and conscientious SRO.

Recommendation

25. Guidance regarding use of the internet and SNS for research of persons and how this might meet the requirement for authorisation as directed surveillance or CHIS should be drawn up and actively disseminated to staff – paragraphs 9, 13, 18 and 19.



Surveillance Inspector



**REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)
POLICY STATEMENT, STRATEGY & GUIDANCE NOTES**

Document Status: Final

Originator: J M Hackett

Updated: J M Hackett

Owner: Solicitor to the Council – Corporate Services

Version: 01.01.03

Date: 17/01/2017

Approved by Audit & Governance Committee

Document Location

This document is held by Tamworth Borough Council, and the document owner is Jane Marie Hackett, Solicitor to the Council – Corporate Services.

Printed documents may be obsolete. An electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
	1.01.01	Scheduled review
December 2008	1.01.02	Scheduled review
September 2010	1.01.03	Scheduled review
September 2011	1.01.04	Scheduled review
December 2012	1.01.05	Scheduled review
November 2014	1.01.06	Scheduled review
April 2015	1.01.07	Scheduled review
February 2016	1.01.08	Scheduled review
January 2017	1.01.09	Scheduled review
October 2017	1.01.09	OSC recommendation

Approvals

Name	Title	Approved
Audit & Governance Committee	Committee Approval	Yes
Council	Council Approval	Yes
CMT	Group Approval	Yes
John Wheatley	Executive Director – Corporate Services	Yes
Jane Marie Hackett	Solicitor to the Council and Monitoring Officer	Yes

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and the website.

TAMWORTH BOROUGH COUNCIL

POLICY & PROCEDURE

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)



Jane Marie Hackett
Solicitor to the Council
Tamworth Borough Council

CONTENTS

	Page No.
Section A Introduction	5 - 6
Section B Effective Date of Operation and Authorising Officer Responsibilities	7 - 8
Section C General Information on RIPA	9
Section D What RIPA Does and Does Not Do	10
Section E Types of Surveillance	11 - 13
Section F Conduct and Use of a Covert Human Intelligence Source (CHIS)	14 - 18
Section G Social Networking Sites	19 - 20
Section H The Role of the RIPA Co-ordinator	21 - 22
Section I Authorisation Procedures	23 - 31
Section J Working with other Agencies	32 - 33
Section K Record Management	34 - 35
Section L Acquisition of Communications Data	36 - 39
Section M Conclusion	40
Appendix 1 A Forms – Directed Surveillance	41
Appendix 2 B Forms – Conduct of a Covert Human Intelligence Source	42
Appendix 3 C Forms – CHIS	43
Annex A Local Authority Procedure	44
Annex B JP Procedure	45
Annex C Application for Judicial Approval and Order Form	46 - 48

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), 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 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.

The Codes of Practice for both Covert Surveillance and Covert Human Intelligence Sources can be obtained by following the link below:

<https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>

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:

[https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition and Disclosure of Communications Data Code of Practice March 2015](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015)

Section B

EFFECTIVE DATE OF OPERATION AND AUTHORISING OFFICER RESPONSIBILITIES

1. The Policy and Procedures in this document have been amended to reflect the latest Codes of Practice which are in force and the legislative amendments which 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 and their guidance documents. 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, when sending copies of any Forms to the Solicitor to the Council (or any other relevant authority), that they are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.
 6. In Accordance with the Codes of Practice, the Senior Responsible Officer (SRO) who is the Solicitor to the Council 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.

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 Operating Officer 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 Operating Officer being satisfied that suitable training on RIPA has been undertaken.
8. 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.
9. Quarterly reports on the use of RIPA will be considered by the Audit and Governance Committee.

DRAFT

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 Ombudsman and/or 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 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 (e.g. 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 as 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. 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.

“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 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.

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 a), b), or c), mentioned above, or which is incidental to anything falling within those sections.

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 Operating Officer, or in his absence, the Deputy Chief Operating Officer 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 Operating Officer, or in his absence, the Executive Director Corporate Services 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 (e.g. 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

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.

Section G

Social Networking Sites

Social networking sites can provide useful information as part of an investigation. However, Council Officers must consider if a RIPA authorisation is required if they are accessing social networking sites for this purpose before undertaking any monitoring of a site.

Whilst initial research of social networking sites to establish a fact or collaborate an intelligence picture is unlikely to require an authorisation for directed surveillance repeat viewing of 'open source' sites may constitute directed surveillance on a case by case basis and this should be borne in mind eg., if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance. The key consideration is whether there is a repeated and systematic collection of personal information.

In addition council officers must be aware that the fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the social networking site being used works. Authorising Officers must not assume that one service provider is the same as another or that the services provided by a single provider are the same. Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available.

The author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered 'open source' and an authorisation is not usually required.

However, repeat viewing of 'open source' sites may constitute directed surveillance on a case by case basis and this should be borne in mind eg., if someone is being monitored through, for example, their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance.

It is necessary and proportionate for the Council to covertly breach access controls, an authorisation for directed surveillance is required. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a Council Officer or by a person acting on the Council's behalf (ie., the activity is more than mere reading of the site's content). It is not unlawful for a Council Officer to set up a false identity, but this must not be done for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws and such photographs must not be used.

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council Officers should be mindful of the following:

- Do not create a false identity in order to 'befriend' individuals on social networks without authorisation under RIPA;
- When viewing an individual's public profile on a social network, do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute an investigation;
- Repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status must only take place under a RIPA authorisation;
- Be aware that it may not be possible to verify the accuracy of information on social networks and if such information is to be used as evidence, take reasonable steps to ensure its validity.

For the avoidance of doubt, only those Officers designated and certified to be 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. Authorisation for directed surveillance can only be granted if it is for the purpose of preventing or detecting crime and the criminal offence is punishable by at least 6 months' imprisonment or it is an offence under sections 146, 147, 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933 (sale of alcohol and tobacco to underage children).

If you are in doubt as to whether or not you can use directed surveillance for the crime you are investigating, you should contact Legal Services for advice.

Section H

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 spread sheet 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 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 date approved by the Magistrate
- 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 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 I

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 Operating Officer	Andrew Barratt
Executive Director Corporate Services	John Wheatley

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 at the earliest opportunity once the specific surveillance is complete. **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 Operating Officer 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 Operating Officer 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 Operating Officer.

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 section 7 of the Children and Young Persons Act 1933 relating to the sale of alcohol 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.

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. In such circumstances seek advice from the RIPA Co-ordinator. There is no requirement for a review form to be submitted to a JP. However if a different surveillance techniques is required it 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

Cancellation should take place at the earliest opportunity.

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;**
 - (ii) **necessary** in the circumstances of the particular case on the ground mentioned
- and**
- (iii) **proportionate** to what it seeks to achieve. (see section on proportionality)

- (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 Operating Officer or in his absence, the Deputy Chief Operating Officer.

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.

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.

Urgent Authorisations

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

Section J

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.

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

DRAFT

Section K

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

The retention of the material obtained during a RIPA operation is governed by the Criminal Procedures Investigations Act (CPIA) 1996 and the Data Protection Act 1998.

Arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance or CHIS. 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 five 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 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 Councils' 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 L

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

In accordance with the Home Office Acquisition and Disclosure of Communications Data Code of Practice the Council is required to have a “the Council Single Point of Contact” is 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. Before an officer can be a SPoC specialist training recognised by the Home Office has to be undertaken. A SPoC must also register his or her details with the Home Office. The Solicitor of the Council is SPoC for Tamworth Borough Council.

Details of the training undertaken is kept in the Central Register.

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 SPoC. If an investigating officer is considering making an application to obtain communications data they should contact the SPoC for advice and to obtain the appropriate forms.

In completing the 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.

As regards “proportionality” there 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. There will only be minimal collateral intrusion in relation to subscriber checks or none will be identified at the time of making the application. 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 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 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 application form it should be passed to the SPoC together with a draft Notice to the Communications Service Provider. If the SPoC is satisfied that the application should proceed, the Application and the draft Notice to the Communications Service Provider will be considered 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 and recorded on the SPoC Log Sheet.

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 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 the Authorising Officer will sign the Notice to the Communication Service Provider, complete the date/time of issue and return all forms to the SPoC

The SPoC will then issue the Notice to the Communications Service Provider

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 M

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:

<https://www.gov.uk/government/collections/ripa-forms--2>

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:

<https://www.gov.uk/government/collections/ripa-forms--2>

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:

<https://www.gov.uk/government/collections/ripa-forms--2>

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

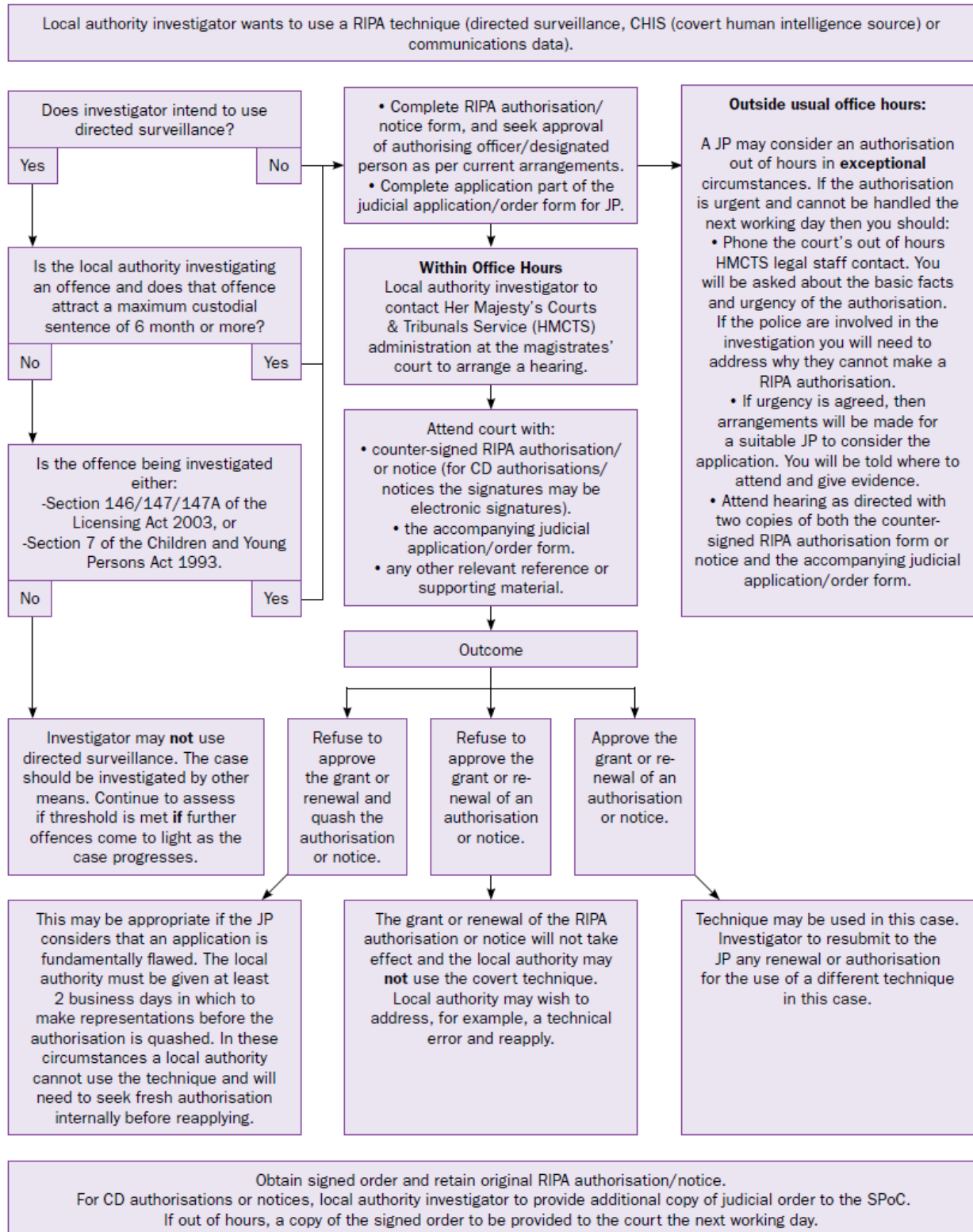
RIPA Section 22 notice to obtain communications data from communications service providers

Reporting an error by a CSP to the IOCCO

Reporting an error by a public authority to the IOCCO

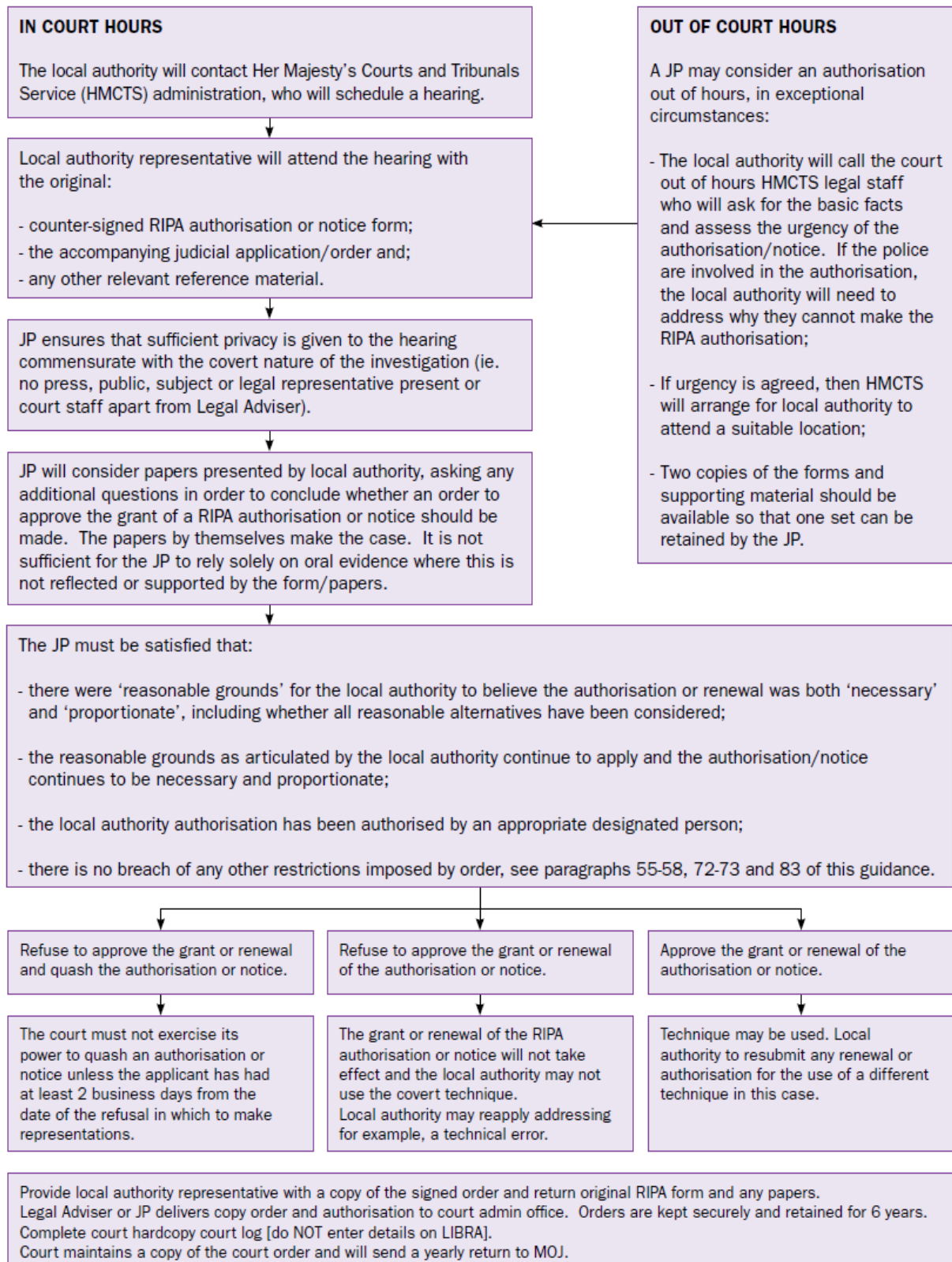
Annex A Local Authority Procedure

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 JP 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 Authority:.....

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:.....

DRAFT

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:

THURSDAY, 26 OCTOBER 2017

REPORT OF THE HEAD OF INTERNAL AUDIT SERVICES

INTERNAL AUDIT UPDATE REPORT 2017/18 QUARTER 2

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 2nd quarter of 2017/18 – 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.

RECOMMENDATIONS

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

EXECUTIVE SUMMARY

The Accounts and Audit Regulations 2015 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 July - September 2017 is set out in the attached document, and the opinion is summarised below.

Audit Opinion.

I am satisfied that sufficient internal audit work has been undertaken to allow us to draw a reasonable conclusion as to the adequacy and effectiveness of the organisation's Risk Management, Control and Governance processes.

Overall in my opinion, based upon the reviews performed during the second quarter of the 2017/18 financial year, the Authority has:

- Adequate and effective risk management arrangements;
- Adequate and effective governance; and
- Adequate and effective control processes.

Specific Issues

No specific issues have been highlighted through the work undertaken by Internal Audit during the second quarter of 2017/18.

RESOURCE IMPLICATIONS

None

LEGAL/RISK IMPLICATIONS BACKGROUND

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

APPENDICES

- Appendix 1 Internal Audit Performance Report 2017/18
- Appendix 2 Percentage of Management Actions Agreed 2017/18
- Appendix 3 Implementation of Agreed Management Actions 2017/18

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 reports on these where possible/necessary. **Appendix 1** shows the progress at the end of 2nd quarter of the year of the work completed against the plan and highlights the work completed. The original audit plan identified 45 audits to be completed in the 2017/18 financial year. The plan has been revised, and a total of 47 audits are now due to be completed by the end of the financial year. At the end of the 2nd quarter of the year, internal audit have commenced/completed 20 audits. This equates to 42% of the revised annual audit plan (specific reviews). In addition to the specific reviews, a total of nine implementation reviews and eight further implementation reviews have been completed for the financial year to date. Three implementations reviews and one further implementation review were completed in the second quarter.

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 2017/18

Twelve audits were finalised within the quarter. **Appendix 2** details the number of recommendations made. A total of 18 recommendations were made in the second quarter with 18 (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. Three first implementation reviews were completed and one second implementation review was completed during the second quarter of 2017/18. **Appendix 3** details the implementation progress to date for the second quarter of the financial year with 35% (21/52) implemented/partially implemented at 1st implementation review. Due to the number of recommendations not implemented at the implementation review, management have been asked to provide assurance and a status update on the outstanding recommendations to date. Management have provided assurance that 94% (49/52) recommendations have now been implemented/partially implemented.

Internal Audit will complete their planned second implementation reviews as timetabled to confirm this. For the second implementation reviews completed, 50% (3/6) of the recommendations were implemented/partially implemented. Two recommendations not implemented at 2nd implementation review were high priority and management have agreed revised implementation dates for all outstanding recommendations. Internal Audit is fairly satisfied with the progress made by management to reduce the level of risk and its commitment to progress the outstanding issues.

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 state 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.

OVERALL CURRENT INTERNAL AUDIT OPINION

I am satisfied that sufficient internal audit work has been undertaken to allow us to draw a reasonable conclusion as to the adequacy and effectiveness of the organisation's Risk Management, Control and Governance processes.

Overall in my opinion, based upon the reviews performed during the second quarter of the 2017/18 financial year, the Authority has:

- Adequate and effective risk management arrangements;
- Adequate and effective governance; and
- Adequate and effective control processes.

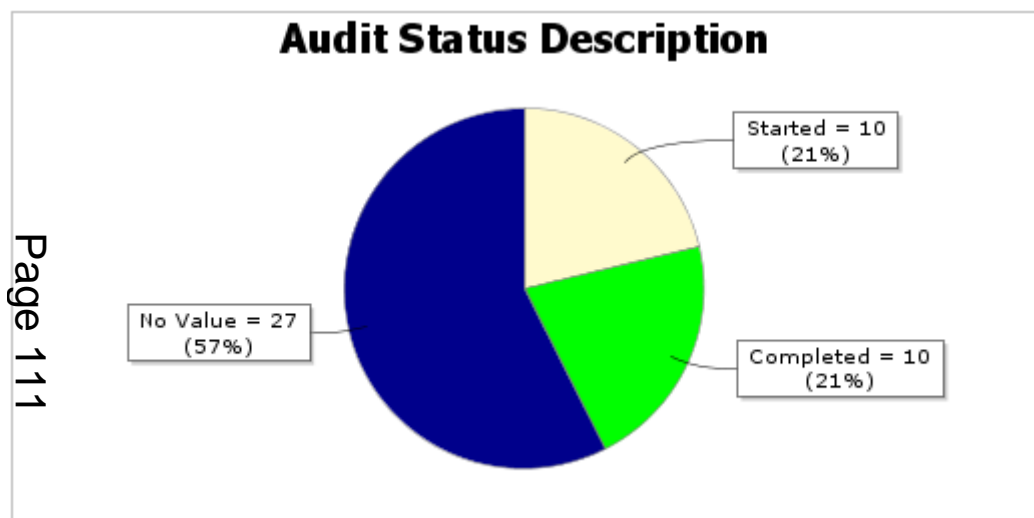
Specific issues:

There were no specific issues highlighted through the work of Internal Audit in the second quarter of the 2017/18 financial year that would need to be highlighted as a corporate risk.

Angela Struthers,
Head of Internal Audit Services

Internal Audit Performance Report 2017/18 Quarter 2 - Revised Plan

Report Type: Audit File Report
 Report Author: Angela Struthers
 Generated on: 04 October 2017



Page 111


Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title	Audit Assurance Level Status Icon
Housing Services	Housing & Health			Risk based review	
Insurance	Finance	✓	Started	System based review	✓
Housing Repairs – Final Accounts	Housing & Health	✓	Completed	Main financial system – interim	
Main Accounting &	Finance			Main financial system –	

Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title	Audit Assurance Level Status Icon
Budgetary Control				full	
Creditors & Procurement – Interim	Finance			Main financial system – interim	
Debtors	Finance			Main financial system – full	
Council Tax	Finance	✔	Started	Main financial system – interim	
NNDR	Finance			Main financial system – interim	
Payroll	Transformation & Corporate Performance			Main financial system – interim	
Bank Reconciliation & Cash Collection	Finance			Main financial system – interim	
Housing & Council Tax Benefits	Finance			Main financial system – interim	
Capital Strategy & Programme Management	Finance			Main financial system – full	
Housing Rents	Housing & Health			Main financial system – interim	
Property Contracts QTR 1	Assets & Environment	✔	Completed	Main financial system – interim	✔
Property Contracts QTR 2	Assets & Environment	✔	Completed	Main financial system – interim	⚠
Property Contracts QTR 3	Assets & Environment			Main financial system – interim	

Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title	Audit Assurance Level Status Icon
Property Contracts QTR 4	Assets & Environment			Main financial system – interim	
Housing Repairs – New Contract	Housing & Health			Additional System Based Review	
Taxi Licences	Assets & Environment	✓	Started	System based review	
Scheme of Delegation	Solicitor & Monitoring Officer	✓	Completed	Risk based review	⚠
Democratic Services business continuity arrangements	Solicitor & Monitoring Officer	✓	Started	System based review	
VAT	Finance	✓	Completed	Risk based review	✓
Corporate Policy Management	Corporate			System based review	
Performance Management	Transformation & Corporate Performance			System based review	
Time Recording & Absence Management	Transformation & Corporate Performance	✓	Started	Risk based review	
Community Wardens – health & safety	Assets & Environment	✓	Started	Risk based review	✓
Equalities	Transformation & Corporate Performance			System based review	
Joint Service Provision/SLA's	Corporate			System based review	
Safeguarding	Solicitor & Monitoring Officer	✓	Started	System based review	

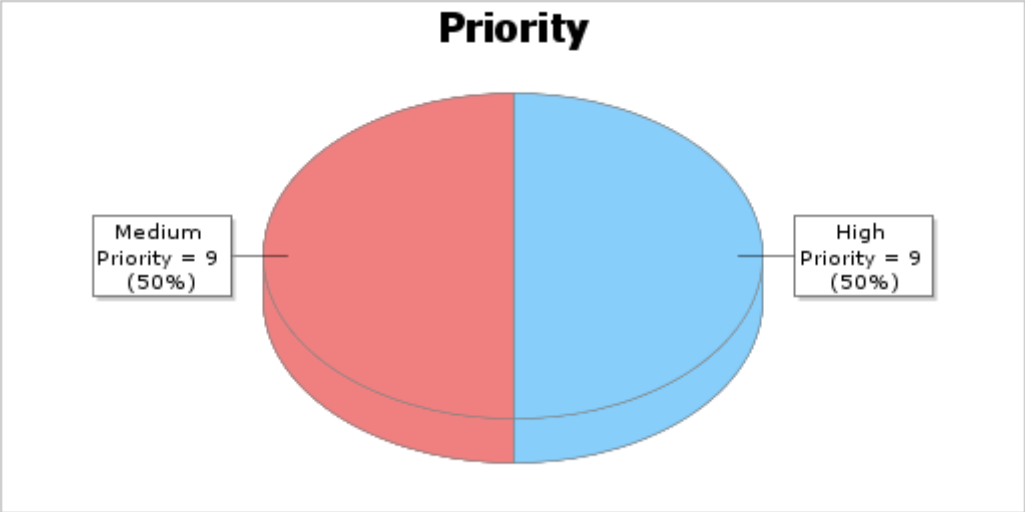
Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title	Audit Assurance Level Status Icon
Emergency Planning	Corporate	✔	Started	System based review	
Network Controls	Technology & Corporate Programmes			Information Technology	
EFin Application Review	Technology & Corporate Programmes			Information Technology	
Websites	Technology & Corporate Programmes			Information Technology	
Orchard Application Review	Technology & Corporate Programmes			Information Technology	
IT Governance	Technology & Corporate Programmes			Information Technology	
Pension Contributions End of year 2016/17	Transformation & Corporate Performance	✔	Completed	Transactional	✔
DFG Testing	Assets & Environment	✔	Started	Transactional	✔
Municipal Charities	Corporate	✔	Completed	Transactional	
Treasury Management QTR 4 2016/17	Finance	✔	Completed	Main financial system – interim	✔
Treasury Management QTR 1 2017/18	Finance	✔	Completed	Main financial system – interim	✔
Treasury Management QTR 2 2017/18	Finance			Main financial system – interim	
Treasury Management QTR 3 2017/18	Finance			Main financial system – interim	
Pension Contributions Interim Testing	Transformation & Corporate Performance	✔	Completed	Transactional	✔

Page 14 of 14

Title	Directorate Description	Audit Status Icon	Audit Status Description	Audit Assurance Type Title	Audit Assurance Level Status Icon
CX Air Application Review	Technology & Corporate Programmes		Started	Information Technology	
Street Scene	Assets & Environment			Risk based review	
Commercial & Industrial Properties	Assets & Environment			Consultancy	
GDPR	Technology & Corporate Programmes			Additional System Based Review	

This page is intentionally left blank

Percentage of Management Actions Agreed 2017/18 Quarter 2

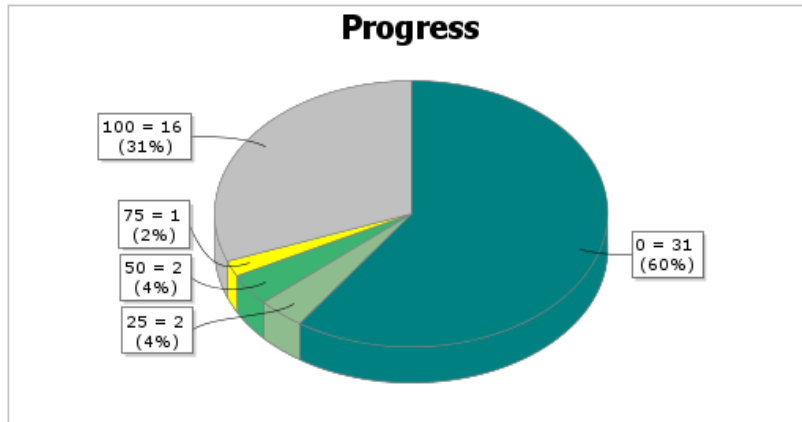


This page is intentionally left blank

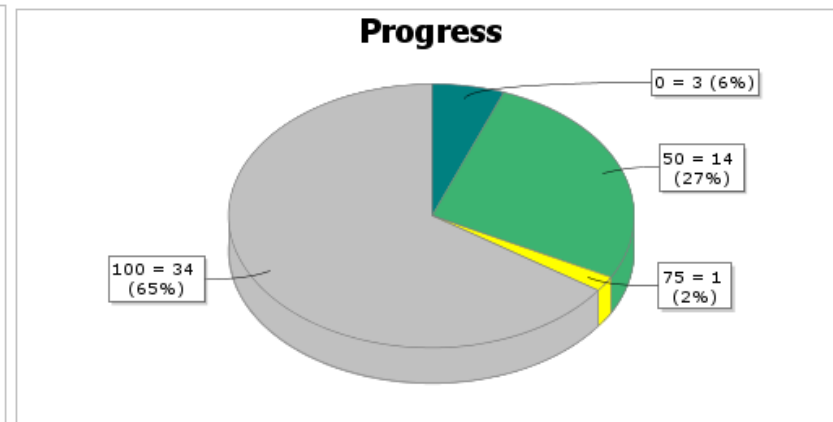
Implementation of Agreed Management Actions 2017/18 Quarter 2

First Implementation Reviews

Status at Implementation Review



Status as at October 2017 – Manager’s Assurance






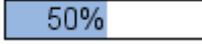

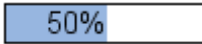
Page 119

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
1617 BS 1.01 Key Holder Records	High Priority	<div style="width: 50%;"><div style="background-color: #4F81BD; height: 10px;"></div></div> 50%	Staffing Resources – Temporary	31-Mar-2018	<div style="width: 100%;"><div style="background-color: #4F81BD; height: 10px;"></div></div> 100%	key holder info now updated and caretakers and admin assistant as well as manager now hold keys for office.
1617 BS 1.04 Alarm Codes	High Priority	<div style="width: 25%;"><div style="background-color: #4F81BD; height: 10px;"></div></div> 25%	Other Higher Priorities	30-May-2018	<div style="width: 50%;"><div style="background-color: #4F81BD; height: 10px;"></div></div> 50%	Completed at depot and castle


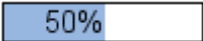

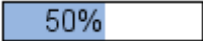


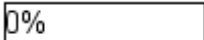
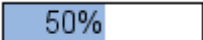








Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
1617 BS 1.05 Building Security Policy	High Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Mar-2018	<input type="text" value="50%"/>	Building use policy is the responsibility of HofCs – Building security has always been under ICT. Building use Policy is to be agreed by CMT.
1617 BS 1.15 Town Hall Security	High Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Mar-2018	<input type="text" value="0%"/>	
1617 BS 2.10 ID Badge – Access Review	High Priority	<input type="text" value="0%"/>	No evidence provided	31-Mar-2018	<input type="text" value="100%"/>	Monthly reports are run and checked and any duplicate or badges that are not required are deactivated.
1617 BS 2.13 Social Services Access	High Priority	<input type="text" value="0%"/>	No evidence provided	31-Mar-2018	<input type="text" value="100%"/>	The only floors that can be restricted are floors 6 & 7. It is the HofCS understanding that if officers and partners need to use the meetings rooms etc they have to have access to all of Marmion House minus floors 6 & 7 which have been isolated and restricted access via ADT.
1617 BS 3.01 Visitor &	High Priority	<input type="text" value="75%"/>	Other Higher	31-Aug-2017	<input type="text" value="75%"/>	

Page 120

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
Contractor Sign In			Priorities			
1617 BS 3.02 Contractor Access	High Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Dec-2017	<input type="text" value="50%"/>	Part of the building use Policy to be approved by CMT.
1617 H&S 2.01 Risk Registers	High Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Aug-2017	<input type="text" value="100%"/>	
1617 H&S 2.03 Fire risk ownership	High Priority	<input type="text" value="0%"/>	Reliance on 3rd Party - Internal	31-Dec-2017	<input type="text" value="100%"/>	The Old TIC is now occupied by a brewing company. The responsibility for risk assessments and fire equipment now sits with the tenant
1617 H&S 3.02 New policy development	High Priority	<input type="text" value="0%"/>	Other Higher Priorities	30-Nov-2017	<input type="text" value="50%"/>	A number of policies and procedures have been updated and will shortly be consulted upon. the updated procedures include: Fire Risk Management, Accident and incident reporting, Control of Substances Hazardous to Health, Display Screen equipment, First Aid, New and Expectant mothers,

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
						Personal Protective Equipment, risk Assessments, Smoking, Suspect packages, Work at heights, violence at Work. Additional procedures will be updated and issued in line with the Health and Safety Action Plan
1617 H&S 4.01 Corporate Training Matrix	High Priority		Other Higher Priorities	31-Dec-2017		The Health and Safety Awareness sessions are advertised on the intranet. A number of awareness sessions are arranged and attendance is co-ordinated by HR to ensure all employees have attended within each 3 year cycle.
1617 H&S 4.03 Premise manager responsibilities	High Priority		Other Higher Priorities	31-Jan-2018		A training course for premise managers is available to be delivered once all premise managers have been identified by HR
1617 H&S 5.01 Safety Audits	High Priority		Other Higher Priorities	31-Mar-2018		A full audit program is in place for 2017/18 whereby all high risk and

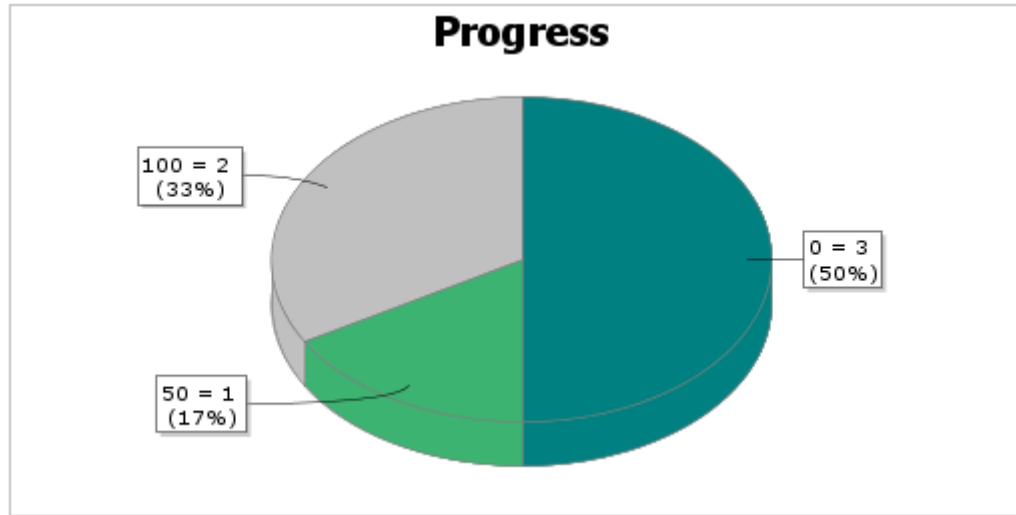
Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
						medium risk services will have undergone an audit by the end of March 2018.
1617 H&S 5.02 Action Programmes	High Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Mar-2018	<input type="text" value="100%"/>	A full service annual action plan is in place for the year 2017/18. The action plan is reviewed by the HS service manager with the HS Advisor
1617 BS 1.02 Key Holder Terms & Conditions	Medium Priority	<input type="text" value="25%"/>	Other Higher Priorities	31-Mar-2018	<input type="text" value="50%"/>	Part of the drafted Building Use Policy – to be approved by CMT
1617 BS 1.08 Carnegie Centre Door Fobs	Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Mar-2018	<input type="text" value="100%"/>	
1617 BS 1.09 Marmion House Key Holders List	Medium Priority	<input type="text" value="0%"/>	No evidence provided	31-Jan-2018	<input type="text" value="100%"/>	Key holders list has been reviewed and key holders sign the list
1617 BS 1.11 Key Checks	Medium Priority	<input type="text" value="0%"/>	No evidence provided	31-Jan-2018	<input type="text" value="100%"/>	
1617 BS 1.14 Key Handling Procedure	Medium Priority	<input type="text" value="0%"/>		31-Jan-2018	<input type="text" value="100%"/>	Currently in the process of finalising policies and procedures which will be in place by the end of this calendar year. There is a process and database in place for recording key

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
						handovers and returns.
1617 BS 2.02 User Access	Medium Priority		Other Higher Priorities	30-Nov-2017		
1617 BS 2.03 Documented Procedures	Medium Priority		No evidence provided	31-Dec-2017		Procedures in place but also included in the building use Policy to be approved by CMT.
1617 BS 2.04 New Starter Forms	Medium Priority		Other Higher Priorities	31-Oct-2017		These are held centrally on the s drive under CST new starter forms.
1617 BS 2.06 ID Badge Terms & Conditions	Medium Priority		No evidence provided	31-Mar-2018		Included as part of the Building Use Policy
1617 BS 2.07 Amendment Requests Retained	Medium Priority		No evidence provided	31-Dec-2017		
1617 BS 2.08 Leaver's ID Badges – Deactivation Process	Medium Priority		No evidence provided	31-Jan-2018		
1617 BS 2.09 Leaver's ID Badge – Deactivated Timely	Medium Priority		No evidence provided	31-Jan-2018		Part of the building policy, however, this is done from the leavers forms.
1617 BS 2.12 ID Badge – Duplicate Entries	Medium Priority		No evidence provided	31-Dec-2017		This was investigated and CCTV have stated that this is a system error. No known reason for the duplications.

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
1617 BS 2.14 Replacement ID Badges	Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Mar-2018	<input type="text" value="50%"/>	Accepted and included in the building use policy to go to CMT.
1617 BS 3.03 Contractor ID Badges	Medium Priority	<input type="text" value="50%"/>	No evidence provided	31-Dec-2017	<input type="text" value="50%"/>	Process implemented, checks to be carried out on a weekly basis.
1617 BS 3.05 Visitor/Contractor Signing In Book	Medium Priority	<input type="text" value="0%"/>	No evidence provided	31-Dec-2017	<input type="text" value="100%"/>	This is part of the security officers evening role.
1617 BS 3.07 Contractor/Visitor ID Swipe Cards	Medium Priority	<input type="text" value="0%"/>	No evidence provided	31-Mar-2018	<input type="text" value="100%"/>	Investigated - unable to complete
1617 BS 4.02 Signed Agreement	Medium Priority	<input type="text" value="0%"/>	No evidence provided	30-Oct-2017	<input type="text" value="0%"/>	
1617 BS 4.03 Licence Agreements	Medium Priority	<input type="text" value="0%"/>	No evidence provided	30-Oct-2017	<input type="text" value="0%"/>	
1617 H&S 3.04 Policy	Medium Priority	<input type="text" value="0%"/>	Other Higher Priorities	31-Aug-2017	<input type="text" value="50%"/>	The Health and Safety Policy is currently being reviewed and it is anticipated only minor changes are expected. Employee responsibilities and processes are likely to remain unchanged. New due date is 31st December 2017

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress at implementation review	Reason Not Implemented	Revised Date for Implementation	Updated status October 2017	Manager Update
1617 H&S 4.02 Training	Medium Priority	0%	Other Higher Priorities	30-Sep-2017	100%	The Health and safety course catalogue is on the intranet and HR send round updates when courses are available.

Second Implementation Reviews 2017/18 Quarter 2



Page 127

Audit Recommendation Code & Title	Recommendation Priority	Recommendation Progress	Original Date for Implementation	Revised Date for Implementation
1617 IM 2.07 Haven: Chip & Pin Devices	High Priority	0%	31-Dec-2016	30-Apr-2018
1617 IM 2.17 Barcode Invoices	High Priority	0%	31-Oct-2016	31-Aug-2017
1617 IM 3.02 Financial Guidance	Medium Priority	0%	30-Sept-2016	30-Sep-2017

This page is intentionally left blank

THURSDAY, 26 OCTOBER 2017

REPORT OF THE HEAD OF INTERNAL AUDIT SERVICES

RISK MANAGEMENT UPDATE

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**
- 2 Endorses the updated Risk Management Policy**

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.

In line with good practice, the Risk Management Policy has been reviewed and updated. Only minor amendments have been made in this review and are shown in the document as attached as **Appendix 2**.

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
Appendix 2 Risk Management Policy















Corporate Risk Register 2017/18

Report Type: Risks Report

Report Author: Angela Struthers

Generated on: 27 September 2017

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 & application of uncertainties of Brexit		12 major - likely		8 major - unlikely	27-Sep-2017
Reputation	Damage to Reputation		9 serious-likely		4 significant-unlikely	27-Sep-2017
Governance & Regulatory Failure	Failure to achieve adequate Governance Standards and statutory responsibilities		9 serious-likely		4 significant-unlikely	27-Sep-2017
Partnership Working and Supply Chain Challenges	Failure in partnership working, shared services or supply chain		9 serious-likely		4 significant-unlikely	27-Sep-2017
Emergency & Crisis Response Threats	Failure to manage an external or internal emergency/disaster situation		9 serious-likely		4 significant-unlikely	27-Sep-2017
Economic Changes	Failure to plan and adapt services to economic changes within the community		6 serious-unlikely		3 serious-very unlikely	27-Sep-2017
Information Management & Information Technology	Failure to secure and manage data and IT infrastructure		12 major - likely		6 serious-unlikely	27-Sep-2017
Loss of Community	Failure to achieve community		12 major - likely		9 serious-likely	27-Sep-2017

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Cohesion	cohesion					
Workforce Planning Challenges	Failure to manage workforce planning challenges		9 serious–likely		4 significant–unlikely	27-Sep-2017
Health & Safety	Failure to manage Health & Safety		12 major – likely		6 serious–unlikely	27-Sep-2017
Corporate Change	Failure to manage corporate change		4 significant–unlikely		4 significant–unlikely	27-Sep-2017
Safeguarding Children & Vulnerable Adults	Failure to safeguard children and vulnerable adults		12 serious – very likely		9 serious–likely	27-Sep-2017
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	27-Sep-2017
Taxi Licences	Taxi Licensing process not followed, giving rise to licenses being issued to persons who are not fit and proper		12 major – likely		4 major – very unlikely	27-Sep-2017
Implementation of response to GDPR Legislation	General Data Protection Regulations (GDPR) coming into effect in May 2018 resulting in significant change for the organisation, including substantial penalties for failing to adhere and breaches		12 major – likely		8 major – unlikely	27-Sep-2017



RISK MANAGEMENT POLICY AND STRATEGY

Document Status: Revised

Originator: A Struthers

Updated: A Struthers

Owner: Executive Director Corporate Services

Version: 01.01.06

Date: 24/08/17

Approved by Audit & Governance Committee

Document Location

This document is held by Tamworth Borough Council, and the document owner is John Wheatley, Corporate Director - Resources.

Printed documents may be obsolete. An electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
April 2010	1.01.01	
18/09/12	1.01.02	Scheduled review
30/3/14	1.01.03	Scheduled review
03/09/15	1.01.04	Scheduled review
03/08/16	1.01.05	Scheduled review
24/08/17	1.01.06	Scheduled review

Approvals

Name	Title	Approved
Audit & Governance Committee	Committee Approval	
CMT	Group Approval	
John Wheatley	Executive Director Corporate Services	
Angela Struthers	Head of Internal Audit Services	Yes

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and the website.

Contents

	Page Number
Risk Management Policy Statement	1
Policy Objectives	3
Risk Management Strategy	3
Risk Appetite	4
Risk Management Roles and Responsibilities	5
Arrangements	6
Risk Management Process	6
Performance Management	7

Risk Management Policy Statement

Statement by the Leader of the Council and Head of Paid Service

The Authority is committed to the culture of Risk Management ensuring that its reputation is not tarnished by an unforeseen event nor is it financially or operationally affected by the occurrence.

It recognises that: -

- Management has the responsibility to plan and systematically approach, the identification, evaluation, and control of risk;
- In order for the Authority to improve risks (opportunities and threats) need to be taken, but they need to be understood and appropriately managed ;
- All Managers and Team Leaders have responsibility for the effective control of risk utilising the support training and resources provided by the Authority;
- The responsibility for insurable losses is management's, not that of an insurance company. Insurance is not a substitute for the management of risk;
- The need to integrate Risk Management into the culture of the Authority.

Risk Management objectives for Tamworth Borough Council are:

- To safeguard the public, members and employees and to protect the Authority's reputation and assets;
- To manage risks in accordance with best practice and ensure risk management is integrated into the culture of Tamworth Borough Council and all those connected with it;
- To identify and take advantage of available opportunities to improve service delivery and/or the Authority's financial position;
- To ensure the Authority delivers its commitments to stakeholders and to demonstrate transparency, accountability and equity in its efforts to do so;
- To anticipate and respond positively to changing social, environmental and legislative requirements; and
- To identify and manage partnership risks.

The Audit & Governance Committee will regularly review the Risk Management Policy and Strategy to ensure their continued relevance to the Borough. They will also assess performance against the aims and objectives.

We attach great significance to Risk Management and it is essential that the Protocol is known and understood by all staff within the Authority. It will form part of the induction training and performance reviews for all staff and members and will be monitored as part of the performance review process utilising the corporate performance system Covalent. We will make adequate resources available to ensure that the commitments made in this statement are achieved.

Risk Management has our total support – it needs yours too for us to succeed.

(Signed)
Head of Paid Service

(Signed)
Leader of the Council

Policy Objectives

In implementing this Policy the Authority will: -

- Identify those assets and exposures which have or may give rise to loss producing events;
- Identify opportunity risks that may give rise to increased benefits
- Maintain detailed 'Risk Registers' of the risks identified as threatening the Authority's operation and document their control on the Authority's Corporate Performance system Covalent;
- Assess the impact of potential loss producing events;
- Take reasonable physical or financial steps to avoid or reduce the impact of potential losses;
- Endeavour to reduce all serious (RED) risks to an acceptable level either by controls or ceasing the activity;
- Ensure that all systems of work reflect the positive risk management culture of the Authority;
- Establish a comprehensive information base of insurable and uninsurable losses;
- Maintain a detailed understanding of insurance;
- Purchase insurance for those risks which cannot be avoided or reduced further, always retaining risks where this is economically attractive.

Risk Management Strategy

The Purpose of this Risk Management Strategy is to effectively manage potential opportunities and threats to the organisation achieving its objectives. The main objectives of the Authority's Risk Management Strategy are to: -

- Achieve continuous improvement in the management of risk;
- Develop a culture that integrates risk management into the day-to-day management process;
- Continue to develop robust systems to identify and evaluate risk;

- Develop reliable performance indicators for target-setting and for making appropriate comparisons;
- Develop systems for performance monitoring to bring about continuous improvements;
- Enabling the Organisation to anticipate and respond to changing social, environmental and legislative conditions;
- Reduce the total cost of risk and mitigate potential future increases in insurance premiums and self-insurance options.

To help achieve these objectives it will be necessary to: -

- Increase the profile of and commitment to Risk Management throughout the Authority;
- Ensure adequate resources (financial and time) are provided;
- To make all partners, providers and delivery agents aware of the Organisation's expectations on risk, both generally as set out in its Risk Management Policy, and where necessary in particular areas of service delivery;
- Develop arrangements to measure performance of Risk Management activities against the aims and objectives;
- Establish clear accountabilities, roles and reporting lines across all services, departments, management and committees;
- Provide for risk assessment in all decision-making processes of the Authority;
- Develop training to build awareness across all levels of activity;
- Performance manage risk management across the Authority.

Risk Appetite

The risk appetite is “the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time” (CIPFA). The Authority will manage the risks by reducing, preventing, transferring, eliminating or accepting the risk.

Whilst the Authority acknowledges that it will have “severe” (red) risks from time to time, it will endeavour to reduce those to an acceptable level either through controls or ceasing the activity (if applicable). Sometimes risks are identified and even though managed, may still remain “severe” (red risk).

Risk Registers must be maintained and managed in the following areas:

Strategic Risks,

Operational Risks,
 Project Risks,
 Partnership Risks,
 Opportunity Risks

“Severe” risks can appear in any of the above risk registers.

Risk Management Roles and Responsibilities

The importance of establishing roles and responsibilities within the risk management framework is pivotal to successful delivery. Considering risks must be embedded into corporate policy approval and operational service delivery.

The agreed roles and responsibilities within the risk management framework are outlined in the table below:

Group /Individual	Role
Corporate Management Team	<ul style="list-style-type: none"> ▪ Provide leadership for the process to manage risks effectively. ▪ Review and revise the Risk Management Policy and Strategy in accordance with the review period. ▪ Monitor and review the Corporate Risk Register on a quarterly basis including the identification of trends, upcoming events and potential new corporate risks.
Audit & Governance Committee	<ul style="list-style-type: none"> ▪ 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. ▪ To monitor the actions being taken to mitigate the impact of potentially serious risks
Cabinet	<ul style="list-style-type: none"> ▪ To provide strategic direction with regard to risk management.
Directors	<ul style="list-style-type: none"> ▪ To provide leadership for the process of managing risks within their directorate. ▪ To ensure that risk management methodology is applied to all service plans, projects, partnerships and proposals within their directorate. ▪ To identify and manage business /operational risks. ▪ To ensure that the management of risk is monitored as part of the performance management process.
Heads of Service	<ul style="list-style-type: none"> ▪ To ensure that all risks are identified, recorded and effectively managed in their area or responsibility. ▪ To review and update their risk register on at least an annual basis but appropriate to the risk.

	<ul style="list-style-type: none"> ▪ To determine the method of controlling the risk. ▪ To delegate responsibility if appropriate for the control of the risk. ▪ To notify the Director of new risks identified for consideration for inclusion on the corporate risk register.
All staff	<ul style="list-style-type: none"> ▪ To ensure that risk is effectively managed in their areas. ▪ To ensure that they notify their managers of new and emerging risks.
Head of Internal Audit Services	<ul style="list-style-type: none"> ▪ To ensure that the risk management strategy is regularly reviewed and updated. ▪ Promote and support the risk management process throughout the Authority. ▪ Advise and assist managers in the identification of risks.

Arrangements

- The Executive Director Corporate Services will ensure that all Managers are aware of their responsibility for Risk Management.
- The Head of Internal Audit Services will be responsible for ensuring that the risk strategy of the Authority is achieved.
- The Operations Accountant will be responsible for the administration of insurance and co-ordination of advice and support.

Risk Management Process

Risk Identification

The identification of risks is completed at various levels and primarily, risks (and opportunities) relate to the achievement of the Authority’s objectives. The objectives can be Strategic, Operational, Project or Opportunity level. This stage can be repeated regularly to ensure that new risks arising are identified and recorded on the risk register as appropriate.

The Authority acknowledges that no one person is responsible for identifying key risks and that they are identified at various levels and various ways.

As a basis, the following risks must be identified:

Those that affect:

- 1 the delivery of the Strategic Plan;
- 2 the operational issues i.e. the delivery of a service;
- 3 the delivery of a project;
- 4 the delivery of a partnership.

Recording Risks

A Risk Register is the primary tool to administer the risks identified. The Covalent system **must** be used to record all corporate, directorate, service, project and partnership risk registers.

As part of business planning, risks are identified. Business plan actions are recorded on the Covalent system under Action Central. Managers should ensure that the associated risks are recorded on the risk register and linked to the appropriate business plan action.

All risks recorded on the risk register should identify the:

- Gross risk,
- Vulnerabilities/causes of the risk,
- Potential effect/consequences of the risk happening,
- Controls in place to reduce the risk,
- Net risk,
- Risk review period.

Reporting Risks

The Corporate Risk Register will be reviewed and updated by the Corporate Management Team on a quarterly basis and then reported to the Audit & Governance Committee.

All reports to any Committee of the Authority require that risks are identified. The Committee report template is set up so that this is completed. It is the duty of the report writer to ensure that the relevant risk register on Covalent is updated to take account of these risks.

Performance Management

The following key performance indicators for the risk management process will be completed.

- The Risk Management Policy and Strategy to be reviewed and updated on an annual basis;
- Corporate Management Team to review and update the corporate risk register taking into account emerging and changing risks on a quarterly basis;
- Risks to be reviewed appropriately to the severity /changing nature of the risk;
- Staff to be appropriately trained in Risk Management and the use of the Covalent system.

THURSDAY, 26 OCTOBER 2017

REPORT OF THE HEAD OF INTERNAL AUDIT SERVICES

COUNTER FRAUD UPDATE

EXEMPT INFORMATION

None

PURPOSE

To provide Members with an update of Counter Fraud work completed during the financial year 2017/18 to date.

RECOMMENDATIONS

That the Committee:

- 1 Considers this report and raises any issue it deems appropriate.**
- 2 Endorses the Fraud & Corruption Policy Statement, Strategy & Guidance Notes. (Appendix 1).**
- 3 Endorses the Whistleblowing Policy (Appendix 2).**
- 4 Endorses the Fraud Risk Register Summary (Appendix 3)**

EXECUTIVE SUMMARY

The Counter Fraud and Corruption Policy Statement, Strategy & Guidance Notes has been reviewed and updated in line with best practice and is attached as **Appendix 1**. There have been no significant changes to the Policy. Within the Strategy, there is the Counter Fraud Work Plan which has been updated for the 2017/18 financial year.

In addition, and in line with best practice, the Whistleblowing Policy has been reviewed and updated and is attached as **Appendix 2**. The review has not identified any significant changes.

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 3**.

Work has progressed on the data matches identified through the National Fraud Initiative (NFI) in the 2016/17 run which was released in February 2016. In total, 1562 matches were identified with 444 of these being recommended for investigation. So far, 1102 of the matches have been processed and cleared and 7 errors have been identified with a total error cost of £4,337 which is being recovered.

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

APPENDICES

Appendix 1 Fraud & Corruption Policy Statement, Strategy & Guidance Notes

Appendix 2 Whistleblowing Policy

Appendix 3 Fraud Risk Register Summary



COUNTER FRAUD AND CORRUPTION POLICY STATEMENT,
STRATEGY & GUIDANCE NOTES

Document Status: Draft

Originator: A Struthers

Updated: A Struthers

Owner: Executive Director – Corporate Services

Version: 01.01.04

Date: 22/08/17

Approved by Audit & Governance Committee

Document Location

This document is held by Tamworth Borough Council, and the document owner is John Wheatley, Executive Director – Corporate Services.

Printed documents may be obsolete. An electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
1/3/12	1.01.01	Scheduled review
30/07/13	1.01.02	Scheduled review
15/08/15	1.01.03	Scheduled review
22/08/17	1.01.04	Scheduled review

Approvals

Name	Title	Approved
Audit & Governance Committee	Committee Approval	
CMT	Group Approval	
TULG	Trade Union Consultation	
John Wheatley	Executive Director – Corporate Services	
Angela Struthers	Head of Internal Audit Services	Yes

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet and the website.

CONTENTS PAGE

	Page
<u>Counter Fraud and Corruption Policy Statement</u>	5
<u>Counter Fraud and Corruption Strategy</u>	
1.0 Introduction	6
2.0 Objectives	9
3.0 Roles and Responsibilities	10
4.0 Culture	10
5.0 Prevention	11
6.0 Detection and Investigation	15
7.0 Recovery, Sanctions & Redress	16
8.0 Training & Awareness	17
9.0 Sharing Information	17
10.0 Implementing the Strategy	18
11.0 Conclusions	18
<u>Counter Fraud and Corruption Guidance Notes</u>	
1.0 Why do we need a Counter Fraud and Corruption Strategy?	19

2.0	Why do we need this advice?	20
3.0	How to recognise a fraud.	21
4.0	How to prevent it.	21
5.0	What to do on suspecting a fraud.	23
5.1	Action by employees	
5.2	Action by managers	
6.0	What happens to the allegation.	24
Appendix 1	The Seven Principles Of Public Life	25
Appendix 2	Statement of Expected Responsibilities	26
Appendix 3	Fraud Response Plan	29
Appendix 4	How to Report any Suspected Frauds, Corruption, Other Irregularities or Concerns.	30

TAMWORTH BOROUGH COUNCIL

COUNTER FRAUD AND CORRUPTION POLICY STATEMENT

- 1.0 Tamworth Borough Council fully recognises its responsibility in relation to the spending of public money (Protecting the Public Purse) and is committed to the fullest support for Councillors and Employees in upholding the reputation of the Council and maintaining public confidence in its integrity. It also recognises its responsibilities under the Proceeds of Crime Act 2002 , Money Laundering Regulations 2007 and the Bribery Act 2010.
- 2.0 The Council acknowledges the threats of fraud and corruption and the harm that they can cause. The Council is committed to maintaining an ethical culture which does not and will not tolerate any form of fraud and corruption. Any such issues will be thoroughly investigated and, if confirmed, dealt with rapidly in the strongest possible way. We will seek the strongest possible sanctions against those who seek to defraud the Council. This includes taking appropriate action against employees, Councillors, contractors, external individuals and organisations.
- 3.0 To deliver the Council's corporate priorities, aims and strategic objectives we need to maximise the financial resources available to us. In order to do this we must reduce the risk of fraud to an absolute minimum.
- 4.0 This Policy Statement, together with the Counter Fraud & Corruption Strategy and Guidance Notes, is intended to provide advice and information to Employees and Councillors but suppliers, contractors and the general public are also encouraged to use this advice and guidance.

Head of Paid Service

Leader of the Council

COUNTER FRAUD AND CORRUPTION STRATEGY

1.0 Introduction

1.1 This strategy is a key element of the Council's overall corporate governance arrangements which aim to ensure the Council is well managed and does the right things, in the right way, for the right people, in a timely, inclusive, open, honest and accountable way. The Council has a range of other interrelated policies and procedures that provide a corporate framework to counter fraud activity. These have been formulated in line with appropriate legislative requirements and include:

- Standing Orders & Financial Regulations,
- National Code of Local Government Conduct,
- Whistleblowing Policy,
- Accounting procedures and records,
- Sound internal control systems,
- Effective Internal Audit,
- Effective recruitment & selection procedures,
- Disciplinary Procedures,
- Fraud Response Plan,
- Benefits Prosecution Policy,
- Data Protection Policy,
- IT Security Policy,
- Personnel Security Policy,
- Physical Security Policy,
- Constitution,
- Scheme of Delegation,
- Members Handbook,
- Code of Corporate Governance,
- Gifts & Hospitality Policy & Register,
- Anti-Money Laundering Policy and Guidance,
- Conflict of Interests Policy,
- Other council procedures as appropriate,
- Any relevant professional Codes of Ethics or obligations.

1.2 All references to fraud within this document include any type of fraud-related offence. Fraud, theft, bribery and corruption are defined as follows:

Fraud – “an intentional false representation, including failure to declare information or abuse of position that is carried out to make gain, cause loss or expose another to the risk of loss.”. The Audit Commission

Theft – “ a person shall be guilty of theft if he/she dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it”. The Theft Act 1968.

Bribery – “A person (“P”) is guilty of an offence if either of the following cases applies.

Case 1 is where—

(a)P offers, promises or gives a financial or other advantage to another person, and

(b)P intends the advantage—

(i)to induce a person to perform improperly a relevant function or activity, or

(ii)to reward a person for the improper performance of such a function or activity.

(3)Case 2 is where—

(a)P offers, promises or gives a financial or other advantage to another person, and

(b)P knows or believes that the acceptance of the advantage would itself constitute the improper performance of a relevant function or activity. (The Bribery Act 2010)

Corruption - “the offering, giving, soliciting or acceptance of an inducement or reward which may influence the action of any person.” (Fraud Audit Manual, the Audit Commission)

1.3 A dishonest act or fraudulent activity may be, but is not limited to, an act or activity that is unethical, improper, or illegal such as:

theft of an asset including, but not limited to, money, tangible property, intellectual property etc;

misappropriation, misapplication, destruction, removal, or concealment of property;

false claims and/or misrepresentation of facts;

alteration or falsification of paper or electronic documents, including the inappropriate destruction of paper or electronic documents;

inappropriate use of computer systems including hacking and software piracy;

embezzlement;

bribery, or corruption of any kind;

unlawful or undeclared conflict of interest;

unauthorised use or misuse of Council property, equipment, materials or records;

- 1.4 Although a dishonest or fraudulent act may have criminal and/or civil law consequences, the Council is not required to use a determination by a criminal or civil body as the basis for determining whether an act is dishonest or fraudulent, nor must the act rise to the level of a crime or violation of civil law in order to constitute a violation of the Council's Conduct and Capability Policy.
- 1.5 The Council also expects that individuals and organisations (e.g. partners, suppliers/contractors and service users) which it comes into contact with, will act towards the Council with integrity and without actions involving fraud or corruption. The Council in turn will endeavour to ensure that all of its dealings will be on the same basis.
- 1.6 In administering its aims and responsibilities the Council is totally committed to deterring fraud and corruption, whether it is attempted on or from within the Council, and is committed to an effective counter fraud and corruption strategy designed to:
- limit, as far as possible, the opportunities to commit fraudulent acts - **prevention**,
 - enable any such acts to be **detected** at an early stage, and
 - deal with any subsequent **investigations** in a prompt, thorough and professional manner.
- 1.7 Overall responsibility for dealing with fraud and corruption rests with the Executive Director Corporate Services, who is the nominated Section 151 Officer having a statutory duty under Section 151 of the Local Government Act 1972 to ensure that there are proper arrangements in place to administer the Council's financial affairs. He is therefore the principal contact for all Councillors and employees.
- 1.8 Internal scrutiny of the Council's various activities occurs as a result of:-
- the Executive Director Corporate Services Section 151 responsibilities and Section 114 Local Government Finance Act 1988 responsibilities,

- the establishment of sound Internal Audit arrangements in accordance with the Accounts and Audit Regulations 2011, and
- the responsibilities placed on the Monitoring Officer under Section 5 of the Local Government and Housing Act 1989.

1.9 External scrutiny of the Council's various activities occurs as a result of involvement by:-

- Local Government Ombudsman,
- External Auditor,
- Central Government Departments and Parliamentary Committees,
- HM Revenues and Customs,
- The Department for Work and Pensions
- The general public.

1.10 This Counter Fraud and Corruption Strategy is based on a series of comprehensive and inter-related procedures designed to deter any attempted fraudulent or corrupt act. These cover:-

- Culture,
- Prevention,
- Detection and Investigation,
- Recovery, Sanction and Redress,
- Training and Awareness,
- Sharing Information,
- Implementing the Strategy.

2.0 Objectives

2.1 The key objectives of this Counter Fraud and Corruption Strategy are to:

Increase awareness of the counter-fraud responsibilities at all levels within and outside the Council;

Further embed and support the effective management of fraud risk within the Council;

Set specific goals for improving the resilience against fraud and corruption through the support of counter-fraud activities across the Council;

Minimise the likelihood and extent of loss through fraud and corruption.

2.2 All of the above will directly support the achievement of the Council priorities whilst ensuring that statutory responsibilities are met.

3.0 Roles and Responsibilities

- 3.1 Roles and responsibilities for identifying and mitigating against the risk of fraud must be clearly understood and embraced effectively.
- 3.2 The risk of fraud and corruption is considered in the Council's corporate risk management arrangements. Chief Officers must therefore ensure that:

Their risk registers accurately reflects the risk of fraud and corruption including any emerging risks;

Controls, including those in a computerised environment and for new systems and procedures, are effective and are properly maintained and documented;

There is compliance with the Council's Financial Regulations and associated guidance, Standing Orders and any other relevant codes of practice;

Those engaged in countering fraud and corruption, have the appropriate authority, skills and knowledge to undertake this work effectively;

That the necessary framework agreements to counter fraud are in place where the Council is working with other organisations either by way of contract or partnership. The Council will not knowingly enter into any contractual agreement with an organisation that fails to comply with its Code of Practice and/or other related procedures.

Findings from fraud investigations lead to relevant system changes.

4.0 Culture

- 4.1 The Council has determined that the culture and ethics of the Authority is one of honesty and openness in all its dealings, with opposition to fraud and corruption. This strategy forms part of the governance arrangements for the authority.
- 4.2 The Council's Councillors and employees play an important part in creating and maintaining this culture. They are encouraged to raise any matters that concern them relating to the Council's methods of operation in accordance with this Counter Fraud & Corruption Strategy or the Council's Whistleblowing Policy.
- 4.3 The Council is committed to driving down Benefit Fraud. Both public perception and organisational culture play key roles in achieving this aim. All Councillors and Employees are therefore required to report

any known material changes affecting Benefit claims to the Department of Works & Pensions(DWP). This specifically includes your own entitlement and of any tenants or sub-tenants that you may have. Failure to do so will result in the Councillor or Employee being subject to the Benefits(CTR) Prosecution Policy and Conduct and Capability Procedures. In addition, it is also a requirement that the timely transfer of information you receive in your normal business activities relating to any other customer who has alerted you to a fact that affects Benefit awards is completed

- 4.4 The Council's Whistleblowing Policy ensures that those raising concerns know they will be treated seriously and properly investigated in a confidential and impartial manner. In raising concerns employees can be assured that they will be protected if the disclosure is made in the public interest and will not affect their employment situation or future prospects with the Council.
- 4.5 Employees can raise their concerns in the first instance with their line manager but where employees feel unable to raise concerns with their immediate line manager/ supervisor they can deal direct with any of the following:-
- the Section 151 Officer (Executive Director Corporate Services),
 - Internal Audit,
 - The Chief Operating Officer
 - the Head of Paid Service,
 - the Monitoring Officer,
 - any member of Corporate Management Team,
 - the External Auditor, or
 - any Trade Union Representative.
- 4.6 Elected Councillors, suppliers, contractors, and the general public are also encouraged to report concerns through any of the above routes.
- 4.7 Unless there are good reasons to the contrary, any allegations received by way of confidential letters or telephone calls will be taken seriously and investigated in an appropriate manner. All concerns will be treated in confidence and every effort will be made not to reveal your identity if you so wish. At the appropriate time, however, you may need to come forward as a witness, but this will be discussed with you, as to whether and how the matter can be proceeded with.
- 4.8 The Nolan Committee set out the seven guiding principles that apply to people who serve the public. The Council will develop our working behaviour around these principles, which are attached as Appendix 1.

5.0 Prevention

5.1 Employees

- 5.1.1 The Council recognises that a key preventative measure in the fight against fraud and corruption is to take effective steps at the recruitment stage to establish, as far as possible, the previous record of potential employees, in terms of their propriety and integrity. In this regard temporary, agency and contract employees should be treated in the same manner as permanent employees. Chief Officers are responsible for ensuring agencies engaged for the supply of temporary employees have rigorous vetting processes and that references are sought direct from previous clients with regard to the suitability and integrity of the candidate.
- 5.1.2 Employee recruitment is required to be in accordance with procedures laid down by the Council. Written references covering the known honesty and integrity of potential employees and where required, evidence of a licence to practice must always be obtained. All qualifications will be verified. There will be an open and fair policy of recruitment with no 'canvassing' or 'favouritism'.
- 5.1.3 Employees of the Council are expected to follow any Code of Conduct relating to their personal Professional Body and also abide by the terms and conditions of employment as set out in the Contract of Employment and the National Scheme of Conditions. The Council will report any known impropriety to the relevant Institution for them to consider appropriate disciplinary action.
- 5.1.4 Employees are reminded that they must comply within Section 117 of the Local Government Act 1972 which requires any interests in contracts that have been or are proposed to be entered into by the Council to be declared. The legislation also prohibits the acceptance of fees or rewards other than by means of proper remuneration. Details are described within the Code of Conduct.
- 5.1.5 Managers are required to observe the formal Conduct and Capability Procedures.
- 5.1.6 All employees are required to declare in a public register (held by the Monitoring Officer) any offers of gifts or hospitality (accepted or not) which are in any way related to the performance of their duties in relation to the Authority. Employees should also declare private work (paid or unpaid) etc., which if permitted must be carried out during hours when not employed on Council work, and should not be

conducted from Council premises or use any Council equipment/assets.

- 5.1.7 The above matters are brought to the attention of employees via induction training and subsequently by internal communications.
- 5.1.8 Management at all levels are responsible for ensuring that employees are aware of the Authority's Financial Regulations and Standing Orders, and that the requirements of each are being met. They are also responsible for ensuring that appropriate procedures are in place to safeguard the resources for which they are responsible, which include accounting control procedures, working manuals and operating procedures. Management must ensure that all employees have access to these rules and regulations and that employees receive suitable training.
- 5.1.9 Managers should strive to create an environment in which employees feel able to approach them with concerns they may have about suspected irregularities. If managers and employees are unsure of the appropriate action they should consult with the Internal Audit Section.

5.2 Councillors

- 5.2.1 Councillors are required to operate within: -
- Sections 49 - 52 of the Local Government Act 2000,
 - Local Authorities (Members' Interest) Regulations 1992 (S.I. 618)
 - The National Code of Local Government Conduct
 - Any local code or amendments agreed and
 - The Council's Standing Orders and Financial Regulations.
- 5.2.2 These matters are specifically brought to the attention of elected Councillors at their induction and subsequent training. Councillors are required to provide the Monitoring Officer with specific information concerning their disclosable pecuniary interests and to keep that information up to date, as required by sections 29-34 of the Localism Act 2011. The Members Interests Register is held by the Monitoring Officer.

5.3 Systems

- 5.3.1 The Council's Scheme of Delegation, Standing Orders and Financial Regulations place a duty on all Councillors and employees to act in accordance with best practice when dealing with the affairs of the Council.

- 5.3.2 The Executive Director Corporate Services has a statutory responsibility under Section 151 of the Local Government Act 1972 to ensure proper administration of financial affairs. Various Codes of Practice outlining systems, procedures and responsibilities are widely distributed to employees.
- 5.3.3 The Internal Audit Section assesses regularly the level of risk within the Council with a view to preventing fraud and corruption. Such assessments are discussed with Chief Officers and, where appropriate, incorporated into work plans.
- 5.3.4 Significant emphasis has been placed on thorough documentation of financial systems, and every effort is made to continually review and develop these systems in line with best practice to ensure efficient and effective internal controls and to include adequate separation of duties. The adequacy and appropriateness of the Council's financial systems are independently monitored by both the Internal Audit Section and External Audit. Any weaknesses identified in internal control will be reported to management whose duty it will be to ensure that corrective action is taken. The Section 151 Officer will use his statutory power to enforce the required changes if necessary.
- 5.3.5 Chief Officers will ensure that internal controls, including those in a computerised environment, are effectively maintained and documented and will investigate any potential weaknesses.
- 5.3.6 Chief Officers must ensure that proportionate counter fraud measures are applied to new systems/procedures.
- 5.3.7 It is evident across the country that an increasingly wide variety of frauds are being perpetrated. The larger frauds may involve the creation of multiple identities and false addresses, and involve different agencies. Employees are therefore encouraged to liaise with those other agencies, exchanging information, where possible and appropriate to help prevent and detect such fraud. It is important that arrangements exist, and are developed, to encourage the exchange of information with other agencies including:-
- other local and statutory authorities,
 - Chief Financial Officer Group,
 - local, regional and national Auditor networks,
 - government departments,
 - police forces,
 - the External Auditor,
 - the National Anti-Fraud Network, and
 - any other Fraud Networks/Forums.
- 5.3.8 The Council has established formal procedures to respond to complaints received about any aspect of service delivery. Issues

relating to fraud and corruption will be passed directly to the Executive Director Corporate Services. Specific guidance has also been issued to all employees in relation to Proceeds of Crime and Money Laundering. The Monitoring Officer acts as the Council's Money Laundering Reporting Officer.

- 5.3.9 The Council will involve the police to prosecute offenders where fraudulent or corrupt acts are discovered. This will be a matter for the Executive Director Corporate Services, Monitoring Officer and the Head of Paid Services to decide, in consultation with the relevant Chief Officer.

6.0 Detection and Investigation

- 6.1 The Council's preventative systems, particularly internal control systems, provide indicators of fraudulent activity and are designed to deter any fraudulent activity.
- 6.2 It is often the alertness of elected Councillors, council employees, and the general public to the possibility of fraud and corruption, that enables detection to occur and appropriate action to take place.
- 6.3 Many frauds are discovered by chance, 'tip-off' or general audit work and arrangements are in place to enable such information to be properly dealt with.
- 6.4 Chief Officers are required by Financial Regulations to report all suspected instances of fraud and corruption to the Executive Director Corporate Services. Early reporting is essential to the success of this strategy, and;
- ensures the consistent treatment of information regarding fraud and corruption,
 - facilitates a thorough investigation of any allegation received by an independent unit (Internal Audit), and
 - ensures maximum protection of the Council's interests.

Suspicious that any transaction or dealing may involve the proceeds of crime should be reported to the Monitoring Officer, who will ensure such suspicions are reported to the appropriate authorities as required by the relevant Act.

- 6.5 The investigating officer will be appointed by the Executive Director Corporate Services. The investigating officer will usually be the Corporate Anti-Fraud Investigations Officer. The investigating officer will;-
- deal promptly and confidentially with the matter,

- have unhindered access to employees, information and other resources as required for investigation purposes
 - record all evidence received,
 - ensure that evidence is sound and adequately supported,
 - ensure security of all evidence collected,
 - liaise as necessary and appropriate with the relevant Chief Officer,
 - liaise as necessary with external agencies e.g. Police,
 - notify the Council's insurers if appropriate.
- 6.6 The Council can be expected to deal swiftly and thoroughly with any employee who attempts to defraud the Council or who is corrupt. The Council will deal positively with fraud and corruption or suspicions thereof. Where appropriate, the Council's disciplinary procedures will be implemented.
- 6.7 There is a need to ensure that any investigation process is not misused and, therefore, any abuse such as raising unfounded malicious allegations may be dealt with as a disciplinary matter.
- 6.8 When it is found that fraud or corruption has occurred due to a break down in the Council's systems or procedures, Chief Officers will ensure that appropriate improvements in systems of control are promptly implemented in order to prevent a reoccurrence.
- 6.9 Depending on the nature and anticipated extent of the allegations, the Internal Audit section will normally work closely with management and other agencies such as the police to ensure that all allegations and evidence is properly investigated and reported upon.
- 6.10 The Council's disciplinary process will be used where the outcome of the Audit Investigation indicates improper behaviour.
- 6.11 The Council will normally wish the police to independently prosecute offenders where financial impropriety is discovered.
- 6.12 Any Councillor who is the subject of allegations of wrong doing can be referred to the Monitoring Officer to the authority (details on the website), who will determine what action should be taken.
- 6.13 All contractors, consultants and organisations receiving funding from the Council who are accused of wrong doing will be the subject of an investigation and where appropriate an independent decision may be taken to terminate the agreement/grant.
- 6.14 The Council's External Auditor has a responsibility to review the Council's arrangements for the prevention, detection and investigation of fraud and corruption and report accordingly.

7.0 Recovery, Sanctions & Redress

7.1 Where the Council identifies fraud then it will:

Recover, prosecute or apply other sanctions to perpetrators, where appropriate.

7.2 Where fraud or corruption by employees is indicated, then action will be taken in accordance with the Council's Conduct and Capability Policy. This may be in addition to any civil recovery action or sanctions.

7.3 The Council aims to be effective in recovering any losses incurred to fraud using, as appropriate, criminal and/or civil law. Success rates will be monitored routinely as an indicator and part of the quality process.

7.4 Wherever possible, redress should be applied. This ensures that the Council is seen as recovering money lost to fraud.

8.0 Training & Awareness

8.1 The Council recognises the importance of training in the delivery of high quality services. The Council supports the concept of fraud awareness training for managers and for employees involved in internal control systems to ensure that their responsibilities and duties in this respect are regularly highlighted and reinforced. Chief Officers are responsible for training employees and promoting awareness of fraud issues.

8.2 Investigation of fraud and corruption centres around the Council's Internal Audit section. Employees engaged in this section, for the detection and prevention of fraud, are properly and regularly trained in all aspects of it. The training plans of the section will reflect this requirement.

8.3 Employees who ignore such training and guidance may face the possibility of disciplinary action.

8.4 Regular training seminars will be provided for Councillors on a wide range of topics including declarations of interest and the Code of Conduct as detailed in the Constitution.

8.5 The Council will maintain an up to date awareness of the types of fraud that it may be exposed to, especially given the ongoing financial situation and the resourcefulness of potential fraudsters. It will review national developments and strengthen systems and procedures accordingly using the following key sources of information:

National Fraud Reports

National Anti-Fraud Network

Midlands Fraud Forum

Local Networking through Staffordshire and the Midlands

Any other sources of fraud awareness/updates etc.

9.0 Sharing Information

- 9.1 The Council is committed to working with other agencies in the detection and prevention of fraud.
- 9.2 Information will be shared internally and with other government departments and other agencies eg insurance companies for the purposes of fraud prevention and detection. This information will be shared in accordance with the principles of the Data Protection Act 1998 and other appropriate legislation.
- 9.3 The Council participates in national data sharing exercises, i.e. the National Fraud Initiative to enable the proactive detection of fraud.

10.0 Implementing the Strategy

- 10.1 Internal Audit will undertake an annual assessment of the effectiveness of existing counter-fraud and corruption arrangements against:
- Fighting Fraud Locally Checklist
 - Other best practice/statutory guidance as required
 - The roles and responsibilities as set out in Appendix 2 of this strategy.
- 10.2 Internal Audit will complete the Counter Fraud Work Plan as detailed in Appendix 5.
- 10.3 Internal Audit will report its findings to the Audit and Governance Committee who will consider the effectiveness of the counter-fraud risk management arrangements.

11.0 Conclusions

- 11.1 The Council's systems, procedures, instructions and guidelines are designed to limit, as far as is practicable, acts of fraud and corruption. All such measures will be kept under constant review to ensure that they keep pace with developments in prevention and detection techniques regarding fraudulent or corrupt activity.
- 11.2 The Council will maintain a continuous review of all its systems and procedures through the Executive Director Corporate Services and Internal Audit, in consultation with the Monitoring Officer where required.

COUNTER FRAUD AND CORRUPTION GUIDANCE NOTES

1.0 Why Do We Need a Counter Fraud And Corruption Strategy?

1.1 Even though the vast majority of people working for the Council are honest and diligent, the Council cannot be complacent. Fraudulent or corrupt acts may include:

System issues	ie where a process/system exists which can be abused by either employees or members of the public (eg Housing Allocations)
Financial issues	ie where individuals or companies have fraudulently obtained money from the Council (eg invalid invoices/work not done)
Equipment issues	ie where Council equipment is used for personal use (eg personal use of council telephones)
Resource issues	ie where there is misuse of resources (eg theft of building materials/cash)
Other issues	ie activities undertaken by officers of the Council which may be: unlawful; fall below established standards or practices; or amount to improper conduct (eg receiving unapproved hospitality)

(This is not an exhaustive list.)

1.2 The prevention of fraud, and the protection of the public purse is **EVERYONE'S BUSINESS**. It is important that all employees know:

- how to recognise a fraud,
- how to prevent it, and
- what to do if they suspect that they have come upon a fraud.

1.3 This guidance has been drawn up to provide information to employees at all levels. The strategy and guidance attempt to assist employees and others with suspicions of any malpractice. The overriding concern is that it is in the public interest for the malpractice to be corrected and, if appropriate, sanctions and redress applied.

1.4 It is important that employees should be able to use any mechanism without fear of victimisation, and fully know that their concerns will be addressed seriously, quickly and discreetly.

1.5 It is important that the whole Council works together to reduce Benefit Fraud. All employees are therefore required to transfer relevant information gathered in their normal day to day activities about possible Benefit irregularities to the Single Fraud Investigation Service (SFIS) at the DWP. So, for example, if during a routine visit/interview you

become aware that a customer is working and “signing on” which they may be entitled to do so but you must tell the SFIS this information. The SFIS will assess the matter and investigate where appropriate. You are not expected to and must not delve any further.

- 1.6 The Council has determined that it should have a culture of honesty and openness in all its dealings, with opposition to fraud and corruption. The Council’s Whistleblowing Policy does this by :-
- making it clear that vigilance is part of the job. Knowingly not raising concerns may be a serious disciplinary offence,
 - recognising that early action may well prevent more worry or more serious loss/damage,
 - making it safe and simple to convey critical information ensuring that any concern in this area is seen as a concern and not a grievance,
 - encouraging information exchange, remembering that there are two sides to every story,
 - providing a way in which concerns can be raised in confidence and not necessarily via the nominated line manager or supervisor,
 - recognising the need for discretion,
 - ensuring the anonymity of the individual, where possible, should this be preferred by the employee, and by protecting employers from reprisals.
- 1.7 Under the Enterprise and Regulatory Reform Act 2013, any disclosure made using the Whistleblowing Policy, within reasonable belief of the worker making the disclosure will only be protected if it is made in the public interest. More detail is found in the Whistleblowing Policy.
- 1.8 There is a need to ensure that any investigation process is not misused and, therefore, any abuse such as raising unfounded malicious allegations may be dealt with as a disciplinary matter.

2.0 Why Do We Need This Advice?

- 2.1 It is important that you follow the advice given and do not try to handle the problem yourself, without expert advice and assistance. A badly managed investigation may do more harm than good. There are a number of internal and external processes which have to be followed to yield a satisfactory conclusion.

3.0 How To Recognise A Fraud

- 3.1 Each employee must be aware of fraud and the areas within their responsibility where fraud may occur.
- 3.2 Fraud can happen wherever employees or independent contractors complete official documentation and can take financial advantage of the Council. The risk of fraud is enhanced where employees or contractors are in positions of trust or responsibility and are not checked or subjected to effective monitoring or validation. Consequently the following areas are susceptible to fraud:-
- claims for work done by independent contractors,
 - travel and expense claims,
 - cash receipts/ petty cash,
 - payroll,
 - ordering, and
 - stocks and assets.
- 3.3 Fraud involves the falsification of records, failing to disclose information or abuse of position. Managers need to be aware of the possibility of fraud when presented with claims/forms/documentation etc. Issues which may give rise to suspicions are:-
- documents that have been altered, “Tippex” used thereon, or different pens and different hand writing,
 - claims that cannot be checked, particularly if prior authorisation was not given,
 - strange trends (use comparisons and reasonableness),
 - confused, illegible text and missing details,
 - delays in documentation, completion or submission, and
 - no vouchers or receipts to support claims.
- 3.4 There are a number of indications of an employee being in a situation whereby they could be acting fraudulently. Common indicators could be:-
- living beyond their means,
 - under financial pressure ,
 - not taking annual leave, and
 - solely responsible for a “risk” area and/or possibly refusing to allow another officer to be involved in their duties and/or have minimal supervision.

4.0 How To Prevent It

- 4.1 By establishing an adverse culture to fraud and corruption the Council can help to prevent its occurrence.
- 4.2 Managers need to :-

- Minimise the opportunity for fraud – this can be achieved by putting in place robust systems of internal controls and checks.
- Reduce the “Pay – Off” – this is achieved by increasing the chances of detection and increasing the penalty for the perpetrator so risks outweigh the benefits of getting “away with it”

4.3 There are 8 basic control types which management should concern themselves with: -

Supervision

Supervisory checks should be completed and recorded by the line manager on the work completed by his/her team.

Organisation

Within each system, there should be policies/procedures setting out how functions should be carried out. There should be clear structures/rules which employees should work within.

Authorisation

Within a system there should be authorisation controls e.g. controls to authorise a payment (electronic/physical signature), and the correct level of authority is used in decision making.

Personnel

There should be clear roles and responsibilities and appropriate level of delegation. The right person should be doing the right job.

Segregation of Duties

Seek to avoid the sole ownership for the processing and control functions of any activity, by one employee.

Physical

This relates to physical controls e.g. access to monies, documents, security of premises etc should be appropriate and restricted where necessary. Where restricted access is necessary, access to keys/door numbers etc should be retained by the person granted access rights. They should not be left on the premises. Inventory checks ensure that assets are controlled.

Arithmetical Accuracy

Checks completed by another person to confirm the accuracy of data input/independent reconciliations of cash floats etc.

Management Functions

Within the system there should be controls for monitoring and reporting upon activity e.g the production of audit trail reports from systems etc. Monitoring to highlight irregularity/non-compliance with rules and procedures and reporting – being accountable for actions.

- 4.4. Employees need to be aware of the possibility of fraud when presented with claims/forms/ documentation, etc. They should also have an awareness of internal rules and procedures; i.e. financial regulations, standing orders, declarations of outside work, hospitality etc.
- 4.5 Deterrence and prevention is the primary aim and if managers implement and control areas as mentioned in 4.3, any deviation from the set procedure should be highlighted in a timely manner.

5.0 What To Do On Suspecting A Fraud

5.1 Action By Employees

- 5.1.1 The Council is committed to the highest possible standards of openness, probity and accountability. Any employee who believes such standards are being breached should report their suspicions. This can be done via the Council's Whistleblowing Policy or you can contact the Executive Director Corporate Services, Internal Audit or a Chief Officer.
- 5.1.2 You should report the matter immediately, make a note of your suspicions and provide as much factual information to support your concerns. Concerns are better raised in writing.
- 5.1.3 The background and the history of the concern, giving names, dates and places where possible, should be set out and the reason why the individual is particularly concerned about the situation. Those who do not feel able to put their concern in writing can telephone or meet the appropriate officer. The earlier the concern is expressed, the easier it is to take action. Individuals may invite their trade union or professional association to raise a matter on their behalf.
- 5.1.4 Do not try to carry out an investigation yourself. This may damage any investigation carried out by the Internal Audit section or an appointed investigator. Help the official investigators by providing information as and when requested and by giving a written statement when required.

5.2 Action By Managers

5.2.1 If managers become suspicious of any action by an employee or supplier or such suspicions are reported to them they should follow these simple rules.

- if possible establish if the irregularity (potential fraud, corruption or error) is a genuine error or possible fraud.
- contact their Chief Officer or any other officer as identified in the Counter Fraud and Corruption Strategy, who will contact the Executive Director Corporate Services or the Internal Audit section.
- contact the Director Transformation & Corporate Performance, where there may be implications under the disciplinary procedures for officers.
- do nothing else, except remain vigilant and await further instructions from the investigating team.

5.2.2 The Council is required to report any cases in which it is suspected that transactions involve the proceeds of crime. If employees or managers have any such suspicion, this should be reported immediately to the Monitoring Officer, who shall advise on the necessary action and ensure the matter is reported to the appropriate authorities.

5.2.3 Details of the relevant contacts can be found in Appendix 4.

6.0 What Happens To The Allegation

6.1 The Executive Director Corporate Services or his investigating officer, will normally carry out a full enquiry even where there is clear evidence of an offence following the Fraud Response Plan (Appendix 3). A full report will be copied and sent to:-

- the relevant Chief Officer, and
- the Head of Paid Service to consider if there needs to be any police involvement.

6.2 It is essential that the Executive Director Corporate Services investigation should be a complete one and the investigating officer to whom it is delegated is entitled to expect the fullest co-operation from all employees.

6.3 A full detailed report on any system control failures and recommended actions to address the failures will be issued to the relevant manager in the format of an internal audit report.

The Seven Principles of Public Life (Nolan Committee)

Selflessness

Holders of public office take decisions in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.

Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.

Objectivity

In carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.

Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

Openness

Holders of public office should be as open as possible about all the decisions and actions that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

Leadership

Holders of public office should promote and support these principles by leadership and example.

Statement of Expected Responsibilities

Stakeholder	Expected Responsibilities
Head of Paid Service	Ultimately accountable as Head of Paid Service for the effectiveness of the Council's arrangements for countering fraud and corruption as well as corporate governance.
Executive Director Corporate Services (Section 151 Officer)	The Executive Director Corporate Services has a statutory duty, under Section 151 of the Local Government Act 1972, Sections 114 and 116 of the Local Government Finance Act 1988 and Accounts and Audit Regulations 2011 to ensure the proper administration of the Council's financial affairs. This includes Internal Audit and Benefit (Council Tax Reduction) Fraud.
Solicitor to the Council (Monitoring Officer)	To advise Councillors and officers on ethical issues, standards and powers to ensure that the Council operates within the Law and Statutory Codes of Practice. The operation of the Council's Money Laundering Policy And Regulation of Investigatory Powers Act (RIPA) 2000 Policies and Procedures. Maintain a Register of Disclosable Pecuniary Interests Maintain a Register of Interests, Gifts & Hospitality.
Director Transformation & Corporate Performance	To put in place a corporate recruitment and selection policy and monitor compliance against it.
Chief Officers	To ensure that fraud and corruption risks are considered as part of the Council's corporate risk management arrangements. To ensure that actions to mitigate risks in this area are effective. To notify the Executive Director Corporate Services of any fraud arising in a timely manner.
Corporate Management Team	Challenge new policies and strategies to ensure that fraud and corruption risks have been taken into account. Review the corporate framework designed to promote an over-riding counter-fraud culture on a

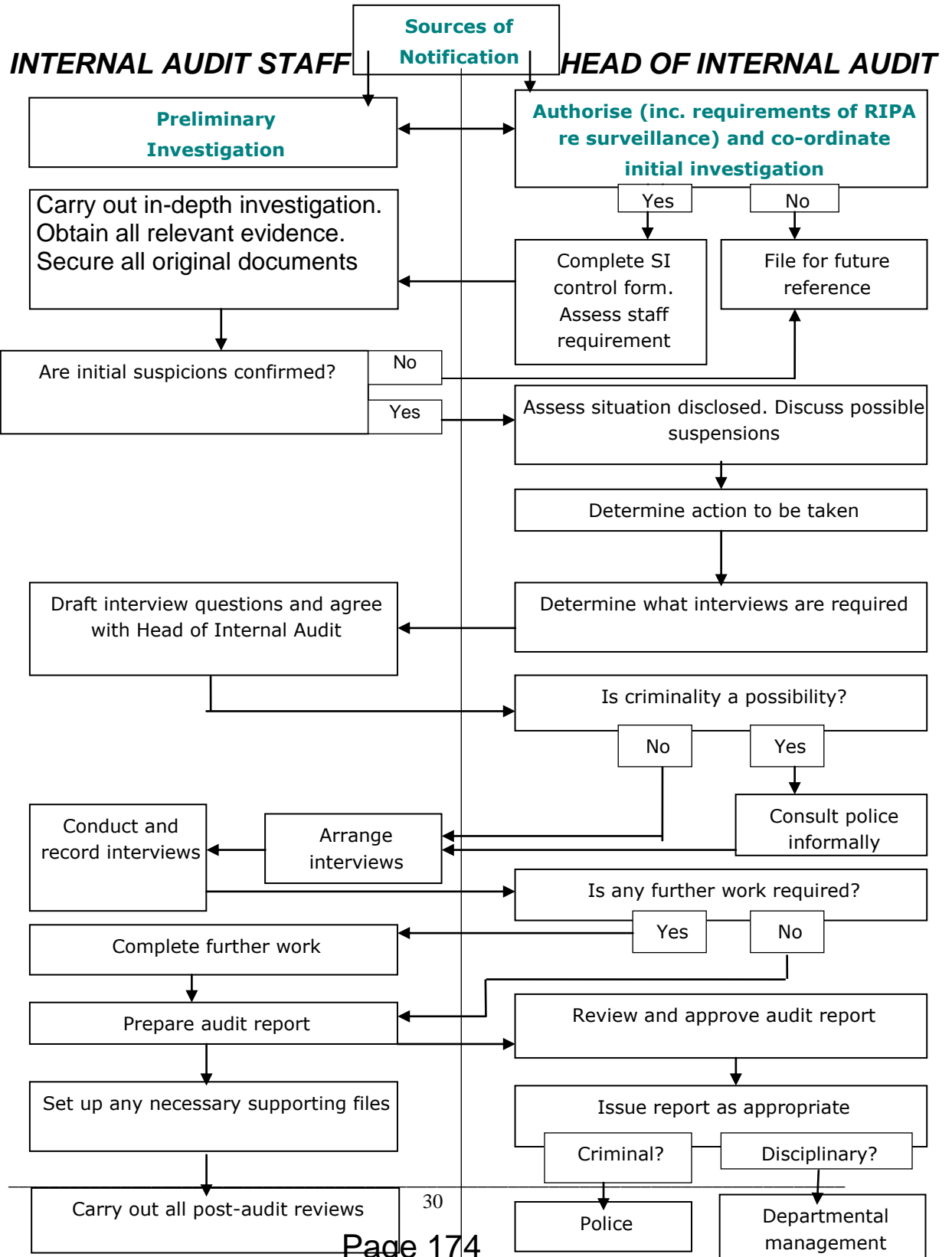
	regular basis. This will include monitoring and evaluating arrangements to ensure effectiveness and compliance with best practice.
Audit and Governance Committee	To monitor the Council's policies and consider the effectiveness of the arrangements for Counter Fraud and Whistleblowing. To exercise all the functions of the Council relating to Codes of Conduct as provided in the Localism Act 2011 except for those functions which under Chapter 7 of the Localism Act 2011 may only be exercised by the full Council.
Deputy leader & Portfolio holder – Assets & Finance	To champion the Council's Counter Fraud & Corruption arrangements and promote them at every opportunity.
Elected Councillors	To support and promote the development of a strong counter fraud culture.
External Audit	Statutory duty to ensure that the Council has in place adequate arrangements for the prevention and detection of fraud, corruption and theft.
Internal Audit	Responsible for developing and implementing the Counter Fraud and Corruption Policy Statement, Strategy and Guidance Notes and investigating any issues reported under this policy. Reporting on the effectiveness of controls to the Audit and Governance Committee. To ensure that all suspected or reported irregularities are dealt with promptly and in accordance with this Strategy and that action is identified to improve controls and reduce the risk of recurrence.
Senior Managers	To promote employee awareness and ensure that all suspected or reported irregularities are immediately referred to Executive Director Corporate Services. To ensure that there are mechanisms in place within their service areas to assess the risk of fraud, corruption and theft and to reduce these risks by implementing robust internal controls.
Employees	To comply with Council policies and procedures, to be aware of the possibility of fraud, corruption and theft, and to report any genuine concerns to the appropriate

	management, the Chief Executive, the Executive Director Corporate Services or Internal Audit.
Public, Partners, Suppliers, Contractors and Consultants	To be aware of the possibility of fraud and corruption against the Council and report any genuine concerns or suspicions. To ensure that effective controls are in place to mitigate risks to the Council.

Tamworth Borough Council

Fraud Response Plan

OPERATIONAL CONTROL



**HOW TO REPORT ANY SUSPECTED FRAUDS, CORRUPTION, OTHER
IRREGULARITIES OR CONCERNS**

To contact Internal Audit Services

Contact: Angela Struthers, Head of Internal Audit Services

Tel: 01827 709234 email: angela-struthers@tamworth.gov.uk

Write to Head of Internal Audit Services (Confidential)
Tamworth Borough Council
Marmion House,
Lichfield Street
Tamworth
B79 7BZ

Or: Andrea Duke, Corporate Anti-Fraud Investigations Officer

Tel: 01827 709541 email: andrea-duke@tamworth.gov.uk

Alternatively you can contact:

John Wheatley, Executive Director Corporate Services

Tel: 01827 709252 email: john-wheatley@tamworth.gov.uk

Jane Hackett, Solicitor to the Council and Monitoring Officer

Tel: 01827 709258 email: jane-hackett@tamworth.gov.uk

Andrew Barratt, Chief Operating Officer

Tel: 01827 709453, email: andrew-barratt@tamworth.gov.uk

Anica Goodwin, Head of Paid Service

Tel: 01827 709225 email: anica-goodwin@tamworth.gov.uk

To contact the Council's external auditor

Write to:

Grant Thornton UK LLP
Colmore Plaza
20 Colmore Circus
Birmingham
West Midlands
B4 6AT

Tel: 0121 212 4000

To report Housing Benefit Fraud contact;

National Benefit Fraud Hotline 0800 854 440 or
text phone number 0800 320 0512 or
Write to NBFH, PO Box No. 224, Preston, PR1 1GP

TAMWORTH BOROUGH COUNCIL INTERNAL AUDIT COUNTER FRAUD WORK PLAN 2017/18

CREATING AN ANTI-FRAUD CULTURE		
OBJECTIVE	RISK	PROGRESS
<p>To build an anti-fraud culture through the adoption of various measures to promote counter fraud awareness by:</p> <ul style="list-style-type: none"> a) Develop & roll out of the e learning package on governance (includes counter fraud & whistleblowing) b) Provide drop in sessions (if required) to staff and members c) Continue to make available counter fraud strategies/policies on the intranet/website 	<p>Failure to make staff, member and the public that their suspicions will be treated confidentially, objectively and professionally. (Medium risk)</p>	<p>E-learning package to be redesigned for new system</p> <p>As required</p> <p>On website and intranet</p>
<p>To complete an annual assessment of whether the level of resource invested to counter fraud and corruption is proportionate for the level of risk.</p>	<p>Failure to make available enough resources for counter fraud work (Medium risk)</p>	<p>March 2018</p>
RESOURCE (DAYS)		25

DETECTING FRAUD		
OBJECTIVE	RISK	PROGRESS
Review communications so that the most effective ways of communicating with staff are utilised.	A lack of robust strategic approach to deterring fraud can undermine actions to build an anti-fraud culture. (Medium risk)	Evaluation and adaptation of National Fraud Authority fraud campaign pack being completed for roll out with E Learning solution
Deter fraud attempts by publishing the organisations counter fraud and corruption stance and the actions it takes against fraudsters.	A lack of understanding as to the stance the authority takes against fraud (Low risk)	Publish Strategy on the intranet and website
Resources (Days)		10

PREVENTING FRAUD		
OBJECTIVE	RISK	PROGRESS
Review the existing Counter Fraud Policy Statement, Strategy and Guidance Notes and update and amend as appropriate.	Out of date policies and procedures which do not cover relevant legislation. (Medium risk)	Annual Review
Review financial guidance and update and amend as appropriate.	Out of date policies and procedures which do not cover relevant legislation. (Medium risk)	Annual Review
Review and update the fraud risk register in line with potential system weaknesses identified during audits or investigations.	Potential risks not identified. (Medium risk)	Completed quarterly
Implement effective Whistleblowing arrangements.	Out of date policies and procedures which do not cover relevant legislation. (Medium risk)	Annual Review
Adopt a Code of Practice for Data Sharing with local partners.	Potential data not identified. (Low risk)	March 2018 – input from ICT
Resources (Days)		15

DETECTING FRAUD		
OBJECTIVE	RISK	PROGRESS
Undertake enquiries as a result of the outcome of the National Fraud Initiative and the Housing Benefit Matching Service	If not undertaken, there is a risk that the opportunity to abuse a system weakness may be heightened as the risk of being caught maybe deemed negligible by the perpetrator. (Medium risk)	On-going
Undertake local proactive exercises through data & intelligence analysis at the Authority as agreed with the Executive Director Corporate Services	If not undertaken, there is a risk that the opportunity to abuse a system weakness may be heightened as the risk of being caught maybe deemed negligible by the perpetrator. (Low risk)	As identified
Review and evaluate the potential for the use of computer aided and other innovative techniques for the detection of fraud.	If not undertaken, there is a risk that fraud could go undetected (Medium risk)	
Resources (Days)		40

INVESTIGATIONS		
OBJECTIVE	RISK	PROGRESS
All referrals will be investigated in accordance with the Counter Fraud and Corruption Policy Statement and Strategy.	<p>The risk of not investigating is that fraud goes unpunished and there is no resulting deterrent effect thus increasing the prevalence of fraud further. (Medium risk)</p> <p>The staff (or others) making the allegation feel they are not taken seriously and referrals cease to be made. (Medium risk)</p>	On-going
		Resources (Days)
		30

SANCTIONS

OBJECTIVE	RISK	PROGRESS
Ensure that the sanctions are applied correctly and consistently (including internal disciplinary, regulatory & criminal.	If sanctions are not imposed there is no deterrence of fraud. (Low risk)	As required
Resources (Days)		

REDRESS

OBJECTIVE	RISK	PROGRESS
<p>Maintain comprehensive records of time spent on each investigation so that this can be included in any compensation claim.</p> <p>Identify and maintain a record of the actual proven amount of loss so that appropriate recovery procedures can be actioned.</p>	<p>Fraudsters may not realise that any and all measures will be taken to recover any money lost to fraud. (Low risk)</p>	<p>As required</p>
Resources (Days)		10

MANDATORY COUNTER FRAUD ARRANGEMENTS (STRATEGIC WORK)		
OBJECTIVE	RISK	PROGRESS
Attendance at relevant fraud forums/meetings to ensure that professional knowledge and skills are maintained.	Failure to ensure the completion of mandatory strategic work may mean that the professional knowledge and skills are not maintained to a high standard.(Medium risk)	On-going
Completion and agreement of work plan.		On-going
Regular meetings with the Executive Director Corporate Services.		On-going
Quarterly report of counter fraud work.		On-going
Attendance at relevant training as required.		On-going
Resources (Days)		10
TOTAL RESOURCES (Days)		140

WHISTLEBLOWING POLICY

Document Status: Draft

Originator: A Struthers

Updated: A Struthers

Owner: Solicitor to the Council & Monitoring Officer

Version: 01.01.04

Date:

Approved by Audit & Governance Committee

Document Location

This document is held by Tamworth Borough Council, and the document owner is Jane Hackett, Solicitor to the Council & Monitoring Officer.

Printed documents may be obsolete. An electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
01/03/12	1.01.01	Scheduled review
29/07/13	1.01.02	Changes under the Enterprise and Regulatory Reform Act 2013
03/08/15	1.01.03	Scheduled review plus changes under The Public Interest Disclosure (Prescribed Persons) Order 2014.
23/08/17	1.01.04	Scheduled review

Approvals

Name	Title	Approved
Audit & Governance Committee	Committee Approval	
CMT	Group Approval	
TULG	Trade Union Consultation	
Jane Hackett	Solicitor to the Council & Monitoring Officer	
Angela Struthers	Head of Internal Audit Services	Yes

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on the Intranet.

WHISTLEBLOWING POLICY

1. Policy Statement

- 1.1 Tamworth Borough Council believes it is important to encourage a climate of openness and dialogue within the Council, where the free expression by staff of their concerns is welcomed by managers as a contribution towards improving services.
- 1.2 Employees are often the first to realise that there may be something seriously wrong within the Council. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the Council. They may also fear harassment or victimisation. In these circumstances it may be easier to ignore the concern rather than report what may just be a suspicion of malpractice.
- 1.3 The Council is committed to the highest possible standards of openness, probity and accountability. In line with that commitment it expects employees, and others that it deals with, who have serious concerns about any aspect of the Council's work to come forward and voice those concerns. It is recognised that most cases will have to proceed on a confidential basis.
- 1.4 This policy document makes it clear that you can do so without fear of victimisation, subsequent discrimination or disadvantage. *This Whistleblowing Policy is intended to encourage and enable anyone to raise concerns in the public interest, in good faith within the Council rather than overlooking a problem or 'blowing the whistle' outside.*

Head of Paid Service

Leader of the Council

2. Introduction

2.1 The Public Interest Disclosure Act 1998 became law in July, 1999. This Act, introduced the protection of whistleblowers and removes the limits of financial liability to which an organisation is exposed should a whistleblower receive unfair treatment. This policy document sets out the Council's response to the requirements of the Act.

2.2 Under the Enterprise and Regulatory Reform Act 2013, any disclosure made using the Whistleblowing Policy, within reasonable belief of the worker making the disclosure will only be protected if it is made in the public interest. It must also show one or more of the following:

(a) that a criminal offence has been committed, is being committed or is likely to be committed,

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur,

(d) that the health or safety of any individual has been, is being or is likely to be endangered,

(e) that the environment has been, is being or is likely to be damaged, or

(f) that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

2.3 This policy is designed for workers. Workers include:

employees;
agency workers;
people that are training with an employer but not employed; and
self-employed workers, if supervised or working off-site.

2.4 Local Government employees have an individual and collective responsibility regarding their conduct and practices, which are always subject to scrutiny. As individuals, employees are required to work within

the Code of Conduct for Tamworth Borough Council Employees and the relevant codes of conduct including the standards appropriate to their professional organisations or associations. The Council's regulatory framework also includes Financial Regulations and Contract Standing Orders that must be met.

- 2.5 All employees have a duty to bring to the attention of management any deficiency in the provision of service and any impropriety or breach of procedure, in accordance with Financial Regulations.”
- 2.6 These procedures are in addition to the Council's complaints procedures including the Grievance Procedure and the Dignity and Respect at Work Policy, and other statutory reporting procedures applying to some Services.
- 2.7 This policy has been discussed with the relevant trade unions and professional organisations and has their support.

3 Aims and Scope of this Policy

- 3.1 This policy aims to:
- encourage you to feel confident in raising concerns that are in the public interest
 - provide avenues for you to raise those concerns and receive feedback on any action taken
 - ensure that you receive a response to your concerns and that you are aware of how to pursue them if you are not satisfied
 - reassure you that you will be protected from possible reprisals or victimisation if you have a reasonable belief that you have made any disclosure in good faith.
- 3.2 There are existing procedures in place to enable you to disclose particular concerns. These are:
- The Authority's Grievance Procedure which enables you to lodge a grievance relating to your own employment;
 - The Authority's Counter Fraud and Corruption Policy Statement, Strategy & Guidance Notes, which outlines how you can disclose potential fraud, bribery, corruption and theft;
 - The Authority's Dignity and Respect at Work Policy, which enables you to disclose cases of potential harassment and bullying;
 - The Authority's Children & Vulnerable Adult Protection Policy (which has its own Whistleblowing Policy in place), for disclosures regarding suspected mistreatment of children and vulnerable adults.

3.3 This policy does **not** replace the corporate complaints procedure or other existing policies for raising issues regarding your employment.

4 Safeguards

4.1 The Council is committed to good practice and high standards and shall be supportive of employees.

4.2 The Council recognises that the decision to report a concern can be a difficult one to make. If what you are saying is within reasonable belief, you should have nothing to fear because you will be doing your duty to your employer and those for whom you are providing a service.

4.3 The Council will not tolerate any harassment or victimisation (including informal pressures) and will take appropriate action to protect you when you raise a concern in good faith. It is a disciplinary matter to victimise a bone fide whistleblower.

5 Confidentiality

5.1 All concerns will be treated in confidence and every effort will be made not to reveal your identity if you so wish. At the appropriate time, however, you may need to come forward as a witness, but this will be discussed with you, as to whether and how the matter can be proceeded with .

6 Anonymous Allegations

6.1 This policy encourages you to put your name to your allegation whenever possible.

6.2 Concerns expressed anonymously are much less powerful but will be considered at the discretion of the Council.

6.3 In exercising this discretion the factors to be taken into account would include:

- the seriousness of the issues raised
- the credibility of the concern; and
- the likelihood of confirming the allegation from attributable sources.

7 Untrue Allegations

- 7.1 If you make an allegation in good faith, but it is not confirmed by the investigation, no action will be taken against you. If, however, you make an allegation frivolously, maliciously or for personal gain, disciplinary action will be taken against you.

8 How to Raise a Concern

- 8.1 As a first step, you should normally raise concerns with your immediate manager or their superior. This depends, however, on the seriousness and sensitivity of the issues involved and who is suspected of the malpractice. For example, if you believe that management is involved, you should approach the Chief Operating Officer, Head of Paid Service, Executive Director Corporate Services, Solicitor to the Council or Head of Internal Audit Services. Where you feel unable to raise the concerns internally due to the nature of the disclosure you should contact the External Auditor who will then ensure that the disclosure is properly investigated.
- 8.2 To raise a concern in respect of Benefits Fraud, you can contact the National Benefit Fraud Hotline - telephone number 0800 854 440 or text phone number 0800 320 0512 or online www.gov.uk/report-benefit-fraud or write to them at NBFH, PO Box No. 224, Preston, PR1 1GP.

9 External contacts

- 9.1 While it is hoped that this policy gives you the reassurance you need to raise such matters internally, it is recognised that there may be circumstances where you can properly report matters to outside bodies, such as prescribed regulators, some of which are outlined at 9.7. If a worker chooses to go to the media, they can expect in most cases to lose their whistleblowing law rights. It is only in exceptional circumstances that a worker can go to the media without losing their rights. The Public Interest Disclosure Act 1998 gives more detail on this.
- 9.2 Concerns may be raised verbally or in writing. Staff who wish to make a written report are invited to use the following format:
- the background and history of the concern (giving relevant dates);
 - the reason why you are particularly concerned about the situation.

- 9.3 The earlier you express the concern the easier it is to take action and you will need to be able to demonstrate to the person contacted that there are reasonable grounds for your concern.
- 9.4 Contact points for advice/guidance on how to pursue matters of concern can be obtained from:
- Chief Operating Officer – 709453
 - Head of Paid Service - 709225
 - Executive Director Corporate Services – 709252
 - Solicitor to the Council & Monitoring Officer – 709258
 - Head of Internal Audit Services – 709234
- 9.5 You may wish to consider discussing your concern with a colleague first and you may find it easier to raise the matter if there are two (or more) of you who have had the same experience or concerns.
- 9.6 You may invite your trade union or professional association representative or a member of staff to be present during any meetings or interviews in connection with the concerns you have raised.
- 9.7 Examples of relevant Prescribed Regulators are as follows:

Proper conduct of public business, value for money fraud and corruption relating to provision of public services	Comptroller and Auditor General
Serious or complex fraud	Director of the Serious Fraud Office
Environmental issues	Environment Agency
Accounting, auditing and actuarial issues	Financial Reporting Council Limited
Health & Safety issues	Health & Safety Executive
Social Housing	Homes & Communities Agency
Data Protection & Freedom of Information	Information Commissioner
Corruption & Bribery	National Crime Agency
Child Welfare & Protection	Children's Commissioner NSPCC

The full list of prescribed regulators can be found in [The Public Interest Disclosure \(Prescribed Persons\) Order 2014](#).

10 How the Council Will Respond

10.1 The Council will always respond to your concerns. Do not forget that testing out your concerns is not the same as either accepting or rejecting them.

10.2 Where appropriate, the matters raised may:

- be investigated by management, internal audit, or through the disciplinary process
- be referred to the police
- be referred to the external auditor
- form the subject of an independent inquiry.

10.3 In order to protect individuals and those accused of misdeeds or possible malpractice, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take. The overriding principle which the Council will have in mind is the public interest. Concerns or allegations which fall within the scope of specific procedures (for example, child protection or discrimination issues) will normally be referred for consideration under those procedures.

10.4 Some concerns may be resolved by agreed action without the need for investigation. If urgent action is required this will be taken before any investigation is conducted.

10.5 Within ten working days of a concern being raised, the Solicitor to the Council will write to you:

- acknowledging that the concern has been received
- indicating how the Council propose to deal with the matter
- giving an estimate of how long it will take to provide a final response
- telling you whether any initial enquiries have been made
- supplying you with information on how the Council will support you if you think this is necessary, whilst the matter is under consideration, and
- telling you whether further investigations will take place and if not, why not.

10.6 The amount of contact between the officers considering the issues and you will depend on the nature of the matter raised, the potential

difficulties involved and the clarity of the information provided. If necessary, the Council will seek further information from you.

- 10.7 Where any meeting is arranged, off-site if you so wish, you can be accompanied by a trade union officer or professional association representative or a member of staff.
- 10.8 The Council accepts that you need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform you of the outcome of any investigation.

11 The Responsible Officer

- 11.1 The Solicitor to the Council & Monitoring Officer has overall responsibility for the maintenance and operation of this policy. That officer maintains a record of concerns raised and the outcomes (but in a form which does not endanger your confidentiality) and will report as necessary to the Council.

12 How the Matter can be Taken Further

- 12.1 If you feel that the Council has not responded correctly at any stage, remember you can go to the other levels and bodies mentioned at paragraph 9.7. While it cannot be guaranteed that all matters will be addressed in the way that you might wish, it will always be the Council's intention to handle the matter fairly and properly. By using this policy, you will help achieve this
- 12.2 If you do take the matter outside the Council, you should ensure that you do not disclose confidential information. Check with the contact point about that.






















This page is intentionally left blank































Fraud & Corruption Risk Register Summary 2017/18






















Report Type: Risks Report



















Report Author: Angela Struthers






















Generated on: 28 September 2017





















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	27-Sep-2017
Assets	Theft of fixed assets		9 serious-likely		4 significant-unlikely	27-Sep-2017
Assets	Theft of Council information/intellectual property		12 major - likely		8 major - unlikely	27-Sep-2017
Assets	Inappropriate use of Council assets for private use		8 significant - very likely		6 significant-likely	27-Sep-2017
Petty cash/imprest accounts	Theft of takings disguised by manipulation of accounts		2 minor-unlikely		2 minor-unlikely	27-Sep-2017
Expenses claims	Inflated claims		6 significant-likely		4 significant-unlikely	27-Sep-2017
Corruption	Disposal of assets - land and property		6 serious-unlikely		3 serious-very unlikely	27-Sep-2017
Corruption	Award of planning consents and licences		9 serious-likely		3 serious-very unlikely	27-Sep-2017
Corruption	Acceptance of gifts, hospitality, secondary employment		6 significant-likely		4 significant-unlikely	27-Sep-2017
Car parking	Theft of takings		9 serious-likely		6 serious-unlikely	27-Sep-2017

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	27-Sep-2017
Money laundering	Using the council to hide improper transactions		8 major – unlikely		4 significant–unlikely	27-Sep-2017
ICT fraud	Improper use of council ICT equipment		12 major – likely		9 serious–likely	27-Sep-2017
Employee – general	Abuse of flexi system Falsification of car loans		6 significant–likely		4 significant–unlikely	27-Sep-2017
Payment of grants to the public	Grants fraudulently claimed		12 major – likely		6 serious–unlikely	27-Sep-2017
Loans & Investments	Misappropriation of funds Fraudulent payment or investment of funds		12 major – likely		4 significant–unlikely	27-Sep-2017
Regeneration Development corruption	Regeneration development corruption		12 major – likely		6 serious–unlikely	27-Sep-2017
Financial statements	The financial statements may be materially mis–stated due to fraud		6 serious–unlikely		4 significant–unlikely	27-Sep-2017
New starter	Fraudulent job application		9 serious–likely		4 significant–unlikely	27-Sep-2017
ICT abuse	Improper use of IT equipment		9 serious–likely		4 significant–unlikely	27-Sep-2017
Benefits fraud – internal	Fraudulent claim by member of staff		9 serious–likely		6 serious–unlikely	27-Sep-2017
Cash theft	Theft of takings disguised by manipulation of accounts		4 significant–unlikely		2 significant–very unlikely	27-Sep-2017
Cash theft	Theft of cash without disguise		4 significant–unlikely		1 minor – very unlikely	27-Sep-2017
Payroll	Payment to non existent employees		2 significant–very unlikely		3 serious–very unlikely	27-Sep-2017
Payroll	Over claiming hours worked		6 significant–likely		2 minor–unlikely	27-Sep-2017

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Payroll	Manipulation of standing data		6 serious–unlikely		2 significant–very unlikely	27-Sep-2017
Assets	Theft of current assets		6 significant–likely		4 significant–unlikely	27-Sep-2017
Procurement & Contract Management						
Selection process	Senior staff influencing junior staff involved in a selection process		6 serious–unlikely		4 significant–unlikely	27-Sep-2017
Lack of awareness of the procurement process	Lack of awareness of risks and issues in the procurement process		6 significant–likely		4 significant–unlikely	27-Sep-2017
Lack of anti fraud culture	No antifraud culture – no due diligence/risk registers		6 significant–likely		2 significant–very unlikely	27-Sep-2017
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	27-Sep-2017
Manipulation of preferred bidders list	Manipulation of preferred bidders list		4 significant–unlikely		2 significant–very unlikely	27-Sep-2017
No formal contract in place	No formal contract in place		8 significant – very likely		6 significant–likely	27-Sep-2017
Prices reworked	Prices reworked to enable the successful bidder to move up the proposal list following initial bidding		6 significant–likely		4 significant–unlikely	27-Sep-2017
Value of contract	Value of contract disaggregated to		12 serious – very likely		6 significant–likely	27-Sep-2017

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
disaggregated	circumvent organisation/EU regulations					
Inappropriate high value purchase	Inappropriate high value purchase for an unauthorised purpose		6 significant–likely		4 significant–unlikely	27-Sep-2017
Inappropriate use of single tender acceptance	Inappropriate use of single tender acceptance		6 significant–likely		4 significant–unlikely	27-Sep-2017
Using agency staff or consultants			4 significant–unlikely		1 minor – very unlikely	27-Sep-2017
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	27-Sep-2017
Contract signing	Contracts signed by member of staff not authorised to do so		12 major – likely		6 serious–unlikely	27-Sep-2017
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	27-Sep-2017
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	27-Sep-2017
Sale of confidential information	A member of staff could disclose information on bids to other contract bidders		12 major – likely		6 serious–unlikely	27-Sep-2017
Creditor payments	Fraudulent requests for creditor payments		9 serious–likely		4 significant–unlikely	28-Sep-2017

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Fraudulent use for one off payment	Staff use the cheque payment process to send to a bogus vendor		6 serious–unlikely		2 significant–very unlikely	28-Sep-2017
Declaration of interests	Lack of declarations of interests		9 serious–likely		4 significant–unlikely	28-Sep-2017
Housing tenancy/homelessness						
Housing allocations	Housing allocated for financial reward fraudulent allocation of property		9 serious–likely		4 significant–unlikely	28-Sep-2017
Illegal sub letting	Illegal sub letting of council property		4 significant–unlikely		2 minor–unlikely	28-Sep-2017
Homelessness	False claim of homelessness		6 significant–likely		2 minor–unlikely	28-Sep-2017
Right to Buy	Fraudulent claim of right to buy discount		6 significant–likely		4 significant–unlikely	28-Sep-2017
Sheltered schemes	Theft of customer monies		4 significant–unlikely		2 significant–very unlikely	27-Sep-2017
Council Tax						
Single Persons Discount	Single persons discount fraudulently claimed		6 significant–likely		6 significant–likely	28-Sep-2017
Discounts/exemptions	Discounts and exemptions falsely claimed		3 minor–likely		2 minor–unlikely	28-Sep-2017
Refund fraud			3 minor–likely		2 minor–unlikely	28-Sep-2017
Suppressed recovery action	Suppressed recovery action		3 minor–likely		2 minor–unlikely	28-Sep-2017
NNDR						
Void exemption	Void exemption falsely claimed		6 significant–likely		4 significant–unlikely	28-Sep-2017

Risk Title	Risk Description	Gross Risk	– Assessment	Current Risk	– Assessment	Last Review Date
Occupation dates	Occupation dates incorrectly notified		6 significant–likely		4 significant–unlikely	28-Sep-2017
Changes to property	Changes to property increase the rateable value		6 significant–likely		4 significant–unlikely	28-Sep-2017
Insurance						
Insurance claims	Claiming for non existent injuries Claiming at another establishment for the same injury overclaiming		9 serious–likely		4 significant–unlikely	28-Sep-2017
Other						
Elections	Fraudulent voting Fraudulent acts by canvassers		12 major – likely		6 serious–unlikely	28-Sep-2017
External funding	Fraudulently claiming/using external funding		1 minor – very unlikely		1 minor – very unlikely	28-Sep-2017
Housing Benefits/Council Tax Reduction Scheme						
Benefits fraud – claimant	Claimant fraudulently claims benefits		12 serious – very likely		8 significant – very likely	28-Sep-2017
Benefits fraud – third party eg landlord	fraudulent claim by third party		4 significant–unlikely		4 significant–unlikely	28-Sep-2017
Cyber						
Cyber risk	Risk of loss, disruption or damage to the reputation of the Authority from some sort of failure of Information Technology systems		6 serious–unlikely		6 serious–unlikely	28-Sep-2017

This page is intentionally left blank

PLANNED REPORTS TO AUDIT AND GOVERNANCE COMMITTEE 2017 - 2018

	Report	Committee Date	Report Of	Comments
1	Role of the Audit Committee	June	Grant Thornton	Presentation/training
2	Audit and Governance Committee Update	June	Grant Thornton	
3	Fee Letter	June	Grant Thornton	
4	Review of the Constitution and Scheme of Delegation for Officers	June	Solicitor to the Council and Monitoring Officer	
5	RIPA Quarterly Report	June	Solicitor to the Council and Monitoring Officer	
6	Members/Standards x 2	June	Solicitor to the Council and Monitoring Officer	
7	Internal Audit Annual and Quarterly Update	June	Head of Internal Audit	
8	Public Sector Internal Audit Standards/Quality Assurance and Improvement Programme	June	Head of Internal Audit	
9	Financial Guidance	June	Head of Internal Audit	
10	Annual Governance Statement and Code of Corporate Governance	June	Head of Internal Audit	

1	Audit Findings Report	July	Grant Thornton	
2	Management Representation Letter	July	Grant Thornton	
3	Annual Statement of Accounts	July	Executive Director Corporate Services	
4	Annual Treasury Outturn	July	Executive Director Corporate Services	
5	RIPA Quarterly Report	July	Solicitor to the Council and Monitoring Officer	
6	Risk Management Quarterly Update	July	Head of Internal Audit	
7	Counter and Corruption Fraud Update	July	Head of Internal Audit	
8	Internal Audit Customer Satisfaction Survey	July	Head of Internal Audit	
9	Internal Audit Quarterly Update	July	Head of Internal Audit	
1	Local Government Ombudsman's Annual Review and Report 2016/17	September	Solicitor to the Council and Monitoring Officer	
1	RIPA Quarterly Update	October	Solicitor to the Council and Monitoring Officer	
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	
1	Audit Report on Certification Work	February	Grant Thornton	
2	Audit Progress Report	February	Grant Thornton	
3	Annual Audit Letter	February	Grant Thornton	
4	RIPA Quarterly Report	February	Monitoring Officer Solicitor to the Council and	
5	Internal Audit Quarterly Update	February	Head of Internal Audit	
6	Risk Management Quarterly Update	February	Head of Internal Audit	
7	Counter Fraud Update	February	Head of Internal Audit	
1	Draft Audit Plan	March	Grant Thornton	
2	Draft Certification Work Plan	March	Grant Thornton	
3	Audit Committee Update	March	Grant Thornton	
4	Auditing Standards	March	Grant Thornton	
5	Informing the Audit Risk Assessment	March	Grant Thornton	
6	Review of the Treasury Management Strategy Statement, Minimum Revenue Provision Policy Statement and Annual Investment Statement	March	Executive Director Corporate Services	

	and the Treasury Management Strategy Statement and Annual Investment Strategy Mid-Year Review Report			
7	Final Accounts – Action Plan	March	Director of Finance	
8	Internal Audit Charter and Audit Plan	March	Head of Internal Audit	
9	Audit and Governance Committee Self-Assessment	March	Head of Internal Audit	
10	Review of Financial Guidance	March	Head of Internal Audit	